PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-152196
(43)Date of publication of application : 24.05.2002

(51)Int.Cl. H04L 9/32
G09C 1/00
H04Q 7/38

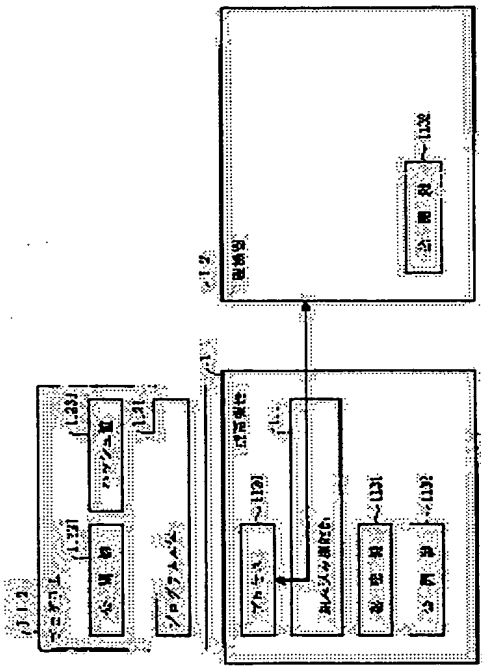
(21)Application number : 2001-250922
(22)Date of filing : 22.08.2001

(30)Priority
Priority number : 2000264850 Priority date : 01.09.2000 Priority country : JP

(71)Applicant : NEC CORP
(72)Inventor : ICHISE NORIYOSHI

(54) METHOD FOR PROGRAM AUTHENTICATION WITHOUT SECRET KEY, PROGRAM ID COMMUNICATION PROCESSING CONTROL METHOD, PROGRAM ID COMMUNICATION RANGE CONTROL METHOD, AND METHOD FOR PROVIDING COMMUNICATION LINE BY OPEN KEY

(57)Abstract:
PROBLEM TO BE SOLVED: To prevent personation of communication in an environment wherein readout and forgery are allowed.
SOLUTION: Portable equipment 11 confirms by a built-in function part 111 that a hash value 11231 is generated by a program main body 1121 and a secret key paired with an open key 11221 indicating the origin of a program 112. Master equipment 12 authenticates the portable equipment 11 by an open key system which uses an open key 11232 and the secret key 1131 and then decides whether or not the program 112 has the authentic origin according to the hash value confirmation result of the portable equipment 11 when the authentication is successful. When the master equipment 12 successfully authenticates the portable equipment 11 and the program 112 has the authentic origin, it is considered that the program 112 is authenticated with the open key 11221.



LEGAL STATUS

[Date of request for examination] 22.08.2001

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－152196
（P2002－152196A）
(43)公開日　平成14年５月24日(2002.5.24)

(51)Int.Cl.'		識別記号	FI		テーマコード'(参考)	
Ｈ０４Ｌ	9/32		Ｇ０９Ｃ	1/00	６４０Ｄ	５Ｊ１０４
Ｇ０９Ｃ	1/00	６４０			６６０Ｄ	５Ｋ０６７
		６６０	Ｈ０４Ｌ	9/00	６７５Ｂ	
Ｈ０４Ｑ	7/38		Ｈ０４Ｂ	7/26	１０９Ｓ	

審査請求　有　　請求項の数35　ＯＬ　（全 43 頁）

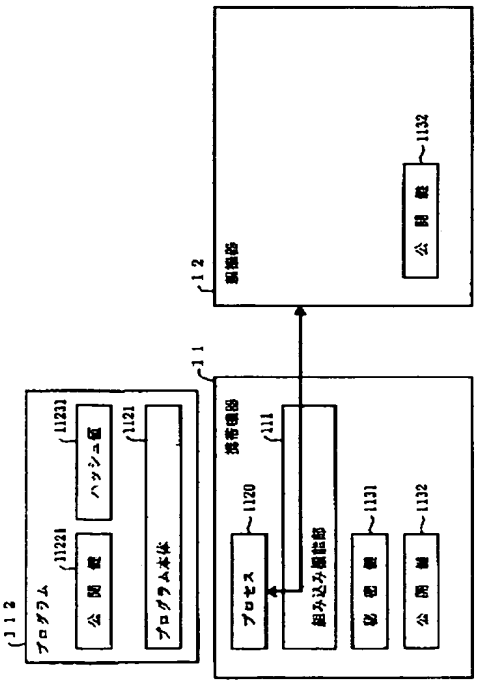
(21)出願番号　特願2001－250922(P2001－250922)
(22)出願日　平成13年８月22日(2001.8.22)
(31)優先権主張番号　特願2000－264850(P2000－264850)
(32)優先日　平成12年９月１日(2000.9.1)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(72)発明者　市瀬　規善
東京都港区芝五丁目７番１号　日本電気株式会社内
(74)代理人　100088890
弁理士　河原　純一

Ｆターム(参考)　5J104 AA07 AA08 AA09 KA02 KA05
KA21 LA03 LA05 LA06 NA02
NA12 PA02
5K067 AA32 BB04 DD17 DD23 EE02
EE10 HH22 HH23 HH24

(54)【発明の名称】　秘密鍵なしプログラム認証方法，プログラムＩＤ通信処理制御方法、プログラムＩＤ通信範囲制御方法および公開鍵毎通信路提供方法

(57)【要約】
【課題】　読み出し改竄可でよい環境での、通信における成りすましを防止する。
【解決手段】携帯機器１１が、組み込み機能部１１１により、ハッシュ値１１２３１がプログラム本体１１２１とプログラム１１２の出所由来を表す公開鍵１１２２１と対をなす秘密鍵とによって生成されたものであることを確認する。親機器１２が、公開鍵１１２３２および秘密鍵１１３１を用いた公開鍵方式により携帯機器１１の認証を行い、認証が成功した場合に、携帯機器１１によるハッシュ値確認結果に基づいてプログラム１１２が真正な出所由来をもつものかを判定する。親機器１２が携帯機器１１の認証に成功し、かつプログラム１１２が真正な出所由来をもつものであるときに、公開鍵１１２２１でプログラム１１２を認証したとする。



【特許請求の範囲】

【請求項１】　プログラムと、該プログラムを元にプロセスを生成し実行するプログラム実行・通信装置と、該プログラム実行・通信装置と通信を行う通信・処理装置とにより構成される情報システムにおいて、前記プログラム実行・通信装置が、該プログラム実行・通信装置に付随する公開鍵および秘密鍵と、前記プログラムを元に生成および実行されるプロセスとを含み、前記プログラムが、プログラム本体と、該プログラムの出所由来を表す公開鍵と、前記プログラム本体に対し該公開鍵と対をなす秘密鍵により行った署名とを含み、前記プログラム実行・通信装置が、前記署名が前記プログラム本体と前記プログラムの出所由来を表す公開鍵と対をなす秘密鍵とによって生成されたものであるかどうかを確認する工程と、前記プログラム実行・通信装置が前記プログラムを元に生成されたプロセスの処理により前記通信・処理装置と通信を行う以前に、前記通信・処理装置が、前記プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により前記プログラム実行・通信装置の認証を行う工程と、前記署名が前記プログラム本体と前記プログラムの出所由来を表す公開鍵と対をなす秘密鍵とによって生成されたものであることが確認できた場合に、前記プログラム実行・通信装置が前記プログラムを元に生成されたプロセスの処理により前記通信・処理装置と通信を行う以前に、前記通信・処理装置が前記プログラムの出所由来を表す公開鍵を得る工程と、前記プログラム実行・通信装置の認証に成功し、かつ前記プログラムの出所由来を表す公開鍵を得られた場合に、前記通信・処理装置が該公開鍵を前記プログラムの出所由来を表すと認証する工程とを含むことを特徴とする秘密鍵なしプログラム認証方法。

【請求項２】　前記プログラム実行・通信装置が、前記署名が前記プログラム本体と前記プログラムの出所由来を表す公開鍵と対をなす秘密鍵とによって生成されたものであるかどうかを確認する工程において、前記署名が前記プログラム本体をハッシュ関数でハッシングしたダイジェストを前記プログラムの出所由来を表す公開鍵と対をなす秘密鍵で暗号化した署名値からなり、前記プログラム実行・通信装置が、前記署名値を前記プログラムの出所由来を表す公開鍵で復号してダイジェストを得るとともに前記プログラム本体をハッシュ関数でハッシングしてダイジェストを得、両ダイジェストが一致するかどうかを判定することを特徴とする請求項１記載の秘密鍵なしプログラム認証方法。

【請求項３】　前記通信・処理装置が、前記プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により前記プログラム実行・通信装置の認証を行う工程において、前記通信・処理装置が、通信してよい相手を示す公開鍵を備え、該通信してよい相手を示す公開鍵と前記プログラム実行・通信装置に付随する公開鍵とが一致するかどうかを判定し、一致する場合に前記プログラム実行・通信装置を認証することを特徴とする請求項１または２記載の秘密鍵なしプログラム認証方法。

【請求項４】　前記通信・処理装置が、前記プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により前記プログラム実行・通信装置の認証を行う工程において、公開鍵によるワン・タイム・パスワード方式が用いられ、前記通信・処理装置は、前記プログラム実行・通信装置にランダムな文字列を送り、前記プログラム実行・通信装置は、該文字列を該プログラム実行・通信装置に付随する秘密鍵で暗号化して前記通信・処理装置に送り返し、前記通信・処理装置は、暗号化された文字列を事前に保持する通信してよい相手を示す公開鍵で復号し、復号した文字列と先に送った文字列とが一致すれば、前記プログラム実行・通信装置を認証することを特徴とする請求項１または２記載の秘密鍵なしプログラム認証方法。

【請求項５】　プログラムと、該プログラムを元にプロセスを生成し実行するプログラム実行・通信装置と、該プログラム実行・通信装置と通信を行う通信・処理装置とにより構成される情報システムにおいて、前記プログラム実行・通信装置が、該プログラム実行・通信装置に付随する公開鍵および秘密鍵と、前記プログラムを元に生成および実行されるプロセスとを含み、前記プログラムが、プログラム本体と、該プログラムの出所由来を表す公開鍵群と、前記プログラム本体および前記公開鍵群を組み合わせて作成されたデータに対し各公開鍵と対をなす各秘密鍵により行った署名群とを含み、前記プログラム実行・通信装置が、各署名が前記プログラム本体および前記公開鍵群を組み合わせて作成されたデータと各署名に対応する各公開鍵と対をなす各秘密鍵とによって生成されたものであるかどうかを確認し、生成されたものであることが確認された署名に対応する公開鍵の集まりを得る工程と、前記プログラム実行・通信装置が前記プログラムを元に生成されたプロセスの処理により前記通信・処理装置と通信を行う以前に、前記通信・処理装置が、前記プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により前記プログラム実行・通信装置の認証を行う工程と、前記生成されたものであることが確認された署名に対応する公開鍵が１つ以上得られた場合に、前記プログラム実行・通信装置が前記プログラムを元に生成されたプロセスの処理により前記通信・処理装置と通信を行う以前に、前記通信・処理装置が前記プログラムの出所由来を表す公開鍵を得る工程と、前記プログラム実行・通信装置の認証に成功し、かつ前記プログラムの出所由来を表す公開鍵を得られた場合に、前記通信・処理装置が、前記プログラム実行・通信装置による署名確認結果の各公開鍵を、前記プログラムの出所由来を表すと認証する工程とを含むこと

を特徴とする秘密鍵なしプログラム認証方法。

【請求項６】　前記プログラム実行・通信装置が、各署名が前記プログラム本体および前記公開鍵群を組み合わせて作成されたデータと各署名に対応する各公開鍵と対をなす各秘密鍵とによって生成されたものであるかどうかを確認し、確認した署名に対応する公開鍵の集まりを得る工程において、各署名が前記プログラム本体および前記公開鍵群の組み合わせで作成されたデータをハッシュ関数でハッシングしたダイジェストを前記プログラムの出所由来を表す各公開鍵と対をなす各秘密鍵で暗号化した各署名値からなり、前記プログラム実行・通信装置が、各署名値を前記プログラムの出所由来を表す各公開鍵でそれぞれ復号してダイジェスト群を得るとともに前記プログラム本体および前記公開鍵群の組み合わせで作成されたデータをハッシュ関数でハッシングしてダイジェストを得、該ダイジェストと前記ダイジェスト群とが一致するかどうかを判定することを特徴とする請求項５記載の秘密鍵なしプログラム認証方法。

【請求項７】　前記通信・処理装置が、前記プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により前記プログラム実行・通信装置の認証を行う工程において、前記通信・処理装置が、通信してよい相手を示す公開鍵を備え、該通信してよい相手を示す公開鍵と前記プログラム実行・通信装置に付随する公開鍵とが一致するかどうかを判定し、一致する場合に前記プログラム実行・通信装置を認証することを特徴とする請求項５または６記載の秘密鍵なしプログラム認証方法。

【請求項８】　前記通信・処理装置が、前記プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により前記プログラム実行・通信装置の認証を行う工程において、公開鍵によるワン・タイム・パスワード方式が用いられ、前記通信・処理装置は、前記プログラム実行・通信装置にランダムな文字列を送り、前記プログラム実行・通信装置は、該文字列を該プログラム実行・通信装置に付随する秘密鍵で暗号化して前記通信・処理装置に送り返し、前記通信・処理装置は、暗号化された文字列を事前に保持する通信してよい相手を示す公開鍵で復号し、復号した文字列と先に送った文字列とが一致すれば、前記プログラム実行・通信装置を認証することを特徴とする請求項５または６記載の秘密鍵なしプログラム認証方法。

【請求項９】　プログラムと、該プログラムを元にプロセスを生成し実行するプログラム実行・通信装置と、該プログラム実行・通信装置と通信を行う通信・処理装置とにより構成される情報システムにおいて、前記プログラムが、プログラム本体と、該プログラムの出所由来を表すＩＤ群とを含み、前記プログラム実行・通信装置が、前記プログラムを元に生成および実行されるプロセスを含み、前記プログラム実行・通信装置が前記プログラムを元に生成されたプロセスの処理により前記通信・処理装置と通信を行う以前に、前記通信・処理装置が、前記プロセスの元となるプログラムの出所由来を表すＩＤ群の一部または全部を得る工程と、前記出所由来を表すＩＤが１つ以上得られたときに、前記通信・処理装置が前記プログラムを元に生成されたプロセスの処理により前記プログラム実行・通信装置と通信を行う工程と、通信によって発生した処理において、前記通信・処理装置が、前記プログラム実行・管理装置から得られた前記出所由来を表すＩＤ群を元にしたアクセス制御を行う工程とを含むことを特徴とするプログラムＩＤ通信処理制御方法。

【請求項１０】　プログラムと、該プログラムを元にプロセスを生成し実行するプログラム実行・通信装置と、該プログラム実行・通信装置と通信を行う通信・処理装置とにより構成される情報システムにおいて、前記プログラムが、プログラム本体，該プログラムの出所由来を表す公開鍵，および該公開鍵と対をなす秘密鍵を含み、前記プログラム実行・通信装置が、前記プログラムを元に生成および実行されるプロセスを含み、前記プログラム実行・通信装置が前記プログラムを元に生成されたプロセスの処理により前記通信・処理装置と通信を行う以前に、前記通信・処理装置が、前記プログラム実行・通信装置から該プログラム実行・通信装置に通信をさせるプロセスの元となる前記プログラムの出所由来を表す公開鍵を得る工程と、前記通信・処理装置が、前記プログラムの出所由来を表す公開鍵および秘密鍵を用いた公開鍵方式により前記プログラムの認証を行う工程と、前記プログラムが認証されたときに、前記通信・処理装置が、前記公開鍵を元にしたアクセス制御により前記プログラム実行・通信装置と通信を行う工程とを含むことを特徴とするプログラムＩＤ通信処理制御方法。

【請求項１１】　前記通信・処理装置が、得られた公開鍵について、前記プログラムの出所由来を表す公開鍵および秘密鍵を用いた公開鍵方式により前記プログラムの認証を行う工程において、公開鍵によるワン・タイム・パスワード方式が用いられ、前記プログラム実行・通信装置が、前記公開鍵を前記通信・処理装置に送り、前記通信・処理装置が、前記プログラム実行・通信装置にランダムな文字列を送り、前記プログラム実行・通信装置が、該文字列を前記秘密鍵で暗号化した文字列を前記通信・処理装置に送り返し、前記通信・処理装置が、暗号化された文字列を前記送られてきた公開鍵で復号し、復号した文字列と先に送った文字列とが一致すれば、前記プログラムを認証することを特徴とする請求項１０記載のプログラムＩＤ通信処理制御方法。

【請求項１２】　プログラムと、該プログラムを元にプロセスを生成し実行するプログラム実行・通信装置と、該プログラム実行・通信装置と通信を行う通信・処理装置とにより構成される情報システムにおいて、前記プロ

グラム実行・通信装置が、該プログラム実行・通信装置に付随する公開鍵および秘密鍵と、前記プログラムを元に生成および実行されるプロセスとを含み、前記プログラムが、プログラム本体と、該プログラムの出所由来を表す公開鍵と、前記プログラム本体に対し該公開鍵と対をなす秘密鍵により行った署名とを含み、前記プログラム実行・通信装置が、前記署名が前記プログラム本体と前記プログラムの出所由来を表す公開鍵と対をなす秘密鍵とによって生成されたものであるかどうかを確認する工程と、前記プログラム実行・通信装置が前記プログラムを元に生成されたプロセスの処理により前記通信・処理装置と通信を行う以前に、前記通信・処理装置が、前記プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により前記プログラム実行・通信装置の認証を行う工程と、前記署名が前記プログラム本体と前記プログラムの出所由来を表す公開鍵と対をなす秘密鍵とによって生成されたものであることが確認できた場合に、前記プログラム実行・通信装置が前記プログラムを元に生成されたプロセスの処理により前記通信・処理装置と通信を行う以前に、前記通信・処理装置が前記プログラムの出所由来を表す公開鍵を得る工程と、前記プログラム実行・通信装置の認証に成功し、かつ前記プログラムの出所由来を表す公開鍵を得られた場合に、前記通信・処理装置が、前記プログラム実行・通信装置から前記プログラムの出所由来を表す公開鍵を得、該公開鍵を元にしたアクセス制御により前記プログラム実行・通信装置と通信を行う工程とを含むことを特徴とするプログラムＩＤ通信処理制御方法。

【請求項１３】　前記プログラム実行・通信装置が、前記署名が前記プログラム本体と前記プログラムの出所由来を表す公開鍵と対をなす秘密鍵とによって生成されたものであるかどうかを確認する工程において、前記署名が前記プログラム本体をハッシュ関数でハッシングしたダイジェストを前記プログラムの出所由来を表す公開鍵と対をなす秘密鍵で暗号化した署名値からなり、前記プログラム実行・通信装置が、前記署名値を前記プログラムの出所由来を表す公開鍵で復号してダイジェストを得るとともに前記プログラム本体をハッシュ関数でハッシングしてダイジェストを得、両ダイジェストが一致するかどうかを判定することを特徴とする請求項１２記載のプログラムＩＤ通信処理制御方法。

【請求項１４】　前記通信・処理装置が、前記プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により前記プログラム実行・通信装置の認証を行う工程において、前記通信・処理装置が、通信してよい相手を示す公開鍵を備え、前記プログラム実行・通信装置に付随する公開鍵と前記通信してよい相手を示す公開鍵とが一致するかどうかを判定することを特徴とする請求項１２または１３記載のプログラムＩＤ通信処理制御方法。

【請求項１５】　前記通信・処理装置が、前記プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により前記プログラム実行・通信装置の認証を行う工程において、公開鍵によるワン・タイム・パスワード方式が用いられ、前記通信・処理装置は、前記プログラム実行・通信装置にランダムな文字列を送り、前記プログラム実行・通信装置は、該文字列を該プログラム実行・通信装置に付随する秘密鍵で暗号化して前記通信・処理装置に送り返し、前記通信・処理装置は、暗号化された文字列を事前に保持する通信してよい相手を示す公開鍵で復号し、復号した文字列と先に送った文字列とが一致すれば、前記プログラム実行・通信装置を認証することを特徴とする請求項１２または１３記載のプログラムＩＤ通信処理制御方法。

【請求項１６】　プログラムと、該プログラムを元にプロセスを生成し実行するプログラム実行・通信装置と、該プログラム実行・通信装置と通信を行う通信・処理装置とにより構成される情報システムにおいて、前記プログラム実行・通信装置が、該プログラム実行・通信装置に付随する公開鍵および秘密鍵と、前記プログラムを元に生成および実行されるプロセスとを含み、前記プログラムが、プログラム本体と、該プログラムの出所由来を表す公開鍵群と、前記プログラム本体および前記公開鍵群を組み合わせて作成されたデータに対し各公開鍵と対をなす各秘密鍵により行った署名群とを含み、前記プログラム実行・通信装置が、各署名が前記プログラム本体および前記公開鍵群を組み合わせて作成されたデータと各署名に対応する各公開鍵と対をなす各秘密鍵とによって生成されたものであるかどうかを確認し、生成されたものであることが確認された署名に対応する公開鍵の集まりを得る工程と、前記プログラム実行・通信装置が前記プログラムを元に生成されたプロセスの処理により前記通信・処理装置と通信を行う以前に、前記通信・処理装置が、前記プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により前記プログラム実行・通信装置の認証を行う工程と、前記生成されたものであることが確認された署名に対応する公開鍵が１つ以上得られた場合に、前記プログラム実行・通信装置が前記プログラムを元に生成されたプロセスの処理により前記通信・処理装置と通信を行う以前に、前記通信・処理装置が前記プログラムの出所由来を表す公開鍵を得る工程と、前記プログラム実行・通信装置の認証に成功し、かつ前記プログラムの出所由来を表す公開鍵を得られた場合に、前記通信・処理装置が、前記プログラム実行・通信装置による署名確認結果の公開鍵の集まりの一部または全部を元にしたアクセス制御により前記プログラム実行・通信装置と通信を行う工程とを含むことを特徴とするプログラムＩＤ通信処理制御方法。

【請求項１７】　前記プログラム実行・通信装置が、各署名が前記プログラム本体および前記公開鍵群を組み合

わせて作成されたデータと各署名に対応する各公開鍵と対をなす各秘密鍵とによって生成されたものであるかどうかを確認する工程において、各署名が前記プログラム本体および前記公開鍵群を組み合わせて作成されたデータをハッシュ関数でハッシングしたダイジェストを前記プログラムの出所由来を表す各公開鍵と対をなす各秘密鍵で暗号化した各署名値からなり、前記プログラム実行・通信装置が、各署名値を各公開鍵でそれぞれ復号した各ダイジェストと、前記プログラム本体および前記公開鍵群を組み合わせて作成されたデータをハッシュ関数でハッシングして得られるダイジェストとが一致するかどうかを判定することを特徴とする請求項１６記載のプログラムＩＤ通信処理制御方法。

【請求項１８】　前記通信・処理装置が、前記プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により前記プログラム実行・通信装置の認証を行う工程において、前記通信・処理装置が、通信してよい相手を示す公開鍵を備え、前記プログラム実行・通信装置に付随する公開鍵と前記通信してよい相手を示す公開鍵とが一致するかどうかを判定することを特徴とする請求項１６または１７記載のプログラムＩＤ通信処理制御方法。

【請求項１９】　前記通信・処理装置が、前記プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により前記プログラム実行・通信装置の認証を行う工程において、公開鍵によるワン・タイム・パスワード方式が用いられ、前記通信・処理装置は、前記プログラム実行・通信装置にランダムな文字列を送り、前記プログラム実行・通信装置は、該文字列を該プログラム実行・通信装置に付随する秘密鍵で暗号化して前記通信・処理装置に送り返し、前記通信・処理装置は、暗号化された文字列を事前に保持する通信してよい相手を示す公開鍵で復号し、復号した文字列と先に送った文字列とが一致すれば、前記プログラム実行・通信装置を認証することを特徴とする請求項１６または１７記載のプログラムＩＤ通信処理制御方法。

【請求項２０】　プログラムと、これらプログラムを元にプロセスをそれぞれ生成し実行する複数のプログラム実行・通信装置とにより構成される情報システムにおいて、前記プログラムが、プログラム本体，および該プログラムの出所由来を表すＩＤ群を含み、あるプログラムを元にあるプログラム実行・通信装置が生成したあるプロセスが、該プログラムまたは別のあるプログラムを元に別のあるプログラム実行・通信装置が生成した別のあるプロセスと通信を行う前に、両プログラム実行・通信装置が、相手プログラム実行・通信装置内のプロセスの元となる前記プログラムの出所由来を表すＩＤ群の一部または全部を得る工程と、前記出所由来を表すＩＤ群が得られたときに、両プログラム実行・通信装置が、得られた出所由来を表すＩＤ群と自プログラム実行・通信装置内のプロセスの元となる前記プログラムの出所由来を表すＩＤ群とを比較し、一致する前記プログラムの出所由来を表すＩＤが１つ以上存在すれば通信路を開く工程とを含むことを特徴とするプログラムＩＤ通信範囲制御方法。

【請求項２１】　プログラムと、各プログラムを元に各プロセスを生成し実行する複数のプログラム実行・通信装置とにより構成される情報システムにおいて、前記プログラムが、プログラム本体，該プログラムの出所由来を表す公開鍵，および該公開鍵と対をなす秘密鍵を含み、あるプログラムを元にあるプログラム実行・通信装置が生成したあるプロセスが、該プログラムまたは別のあるプログラムを元に別のあるプログラム実行・通信装置が生成した別のあるプロセスと通信を行う前に、両プログラム実行・通信装置が、相手プログラム実行・通信装置から相手プログラム実行・通信装置内のプロセスの元となる前記プログラムの出所由来を表す公開鍵をそれぞれ得る工程と、両プログラム実行・通信装置が、相手プログラム実行・通信装置から得られた公開鍵と自プログラム実行・通信装置内のプロセスの元となる前記プログラムの出所由来を表す公開鍵とが一致するかどうかを判定する工程と、両プログラム実行・通信装置が、相手プログラム実行・通信装置内のプロセスの元となる前記プログラムの出所由来を表す公開鍵および秘密鍵を用いて相手プログラム実行・通信装置内のプロセスの元となるプログラムの相互認証を行う工程と、相手プログラム実行・通信装置から得られた公開鍵と自プログラム実行・通信装置内のプロセスの元となる前記プログラムの出所由来を表す公開鍵とが一致し、かつ相手プログラム実行・通信装置内のプロセスの元となるプログラムが相互認証されたときに、両プログラム実行・通信装置が通信路を開く工程とを含むことを特徴とするプログラムＩＤ通信範囲制御方法。

【請求項２２】　両プログラム実行・通信装置が、相手プログラム実行・通信装置内のプロセスの元となる前記プログラムの出所由来を表す公開鍵および秘密鍵を用いて相手プログラム実行・通信装置内のプロセスの元となるプログラムの相互認証を行う工程において、公開鍵によるワン・タイム・パスワード方式が用いられ、両プログラム実行・通信装置が、自プログラム実行・通信装置に付随する公開鍵を相手プログラム実行・通信装置に送り、相手プログラム実行・通信装置にランダムな文字列をそれぞれ送り、相手プログラム実行・通信装置が、該文字列を相手プログラム実行・通信装置内のプロセスの元となる前記プログラムの出所由来を表す公開鍵と対をなす秘密鍵で暗号化した文字列を自プログラム実行・通信装置に送り返し、自プログラム実行・通信装置が、暗号化された文字列を対応する公開鍵で復号し、復号した文字列と先に送った文字列とが一致すれば、相手プログラム実行・通信装置通信装置内のプロセスの元となるプ

ログラムを認証することを特徴とする請求項２１記載のプログラムＩＤ通信範囲制御方法。

【請求項２３】　プログラムと、各プログラムを元に各プロセスを生成し実行する複数のプログラム実行・通信装置とにより構成される情報システムにおいて、前記プログラム実行・通信装置が、自プログラム実行・通信装置に付随する公開鍵および秘密鍵と、相手プログラム実行・通信装置に付随する公開鍵と、前記プログラムを元に生成および実行されるプロセスとを含み、前記プログラムが、プログラム本体と、該プログラムの出所由来を表す公開鍵と、前記プログラム本体に対し該公開鍵と対をなす秘密鍵により行った署名とを含み、あるプログラムを元にあるプログラム実行・通信装置が生成したあるプロセスが、該プログラムまたは別のあるプログラムを元に別のあるプログラム実行・通信装置が生成した別のあるプロセスと通信を行う前に、両プログラム実行・通信装置が、前記署名が前記プログラム本体と前記プログラムの出所由来を表す公開鍵と対をなす秘密鍵とによって生成されたものであるかどうかを確認する工程と、前記通信を行う前に、両プログラム実行・通信装置が、相手プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により相手プログラム実行・通信装置の認証を行う工程と、両プログラム実行・通信装置が、前記署名が前記プログラム本体と前記プログラムの出所由来を表す公開鍵と対をなす秘密鍵とによって生成されたものであることが確認できた場合に、前記通信を行う前に、前記公開鍵を相手プログラム実行・通信装置に伝える工程と、両プログラム実行・通信装置が、相手プログラム実行・通信装置から得られた公開鍵と自プログラム実行・通信装置内のプロセスの元となる前記プログラムの出所由来を表す公開鍵とが一致するかどうかを判定する工程と、相手プログラム実行・通信装置内のプロセスの元となるプログラムが相互認証され、かつ相手プログラム実行・通信装置から得られた公開鍵と自プログラム実行・通信装置内のプロセスの元となる前記プログラムの出所由来を表す公開鍵とが一致したときに、両プログラム実行・通信装置が通信路を開く工程とを含むことを特徴とするプログラムＩＤ通信範囲制御方法。

【請求項２４】　両プログラム実行・通信装置が、前記署名が前記プログラム本体と前記プログラムの出所由来を表す公開鍵と対をなす秘密鍵とによって生成されたものであるかどうかを確認する工程において、前記署名が前記プログラム本体をハッシュ関数でハッシングしたダイジェストを前記プログラムの出所由来を表す公開鍵と対をなす秘密鍵で暗号化した署名値からなり、両プログラム実行・通信装置が、前記署名値を前記プログラムの出所由来を表す公開鍵で復号してダイジェストを得るとともに前記プログラム本体をハッシュ関数でハッシングしてダイジェストを得、両ダイジェストが一致するかどうかを判定することを特徴とする請求項２３または２４記載のプログラムＩＤ通信範囲制御方法。

【請求項２５】　両プログラム実行・通信装置が、相手プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により相手プログラム実行・通信装置の認証を行う工程において、両プログラム実行・通信装置が、通信してよい相手を示す公開鍵を備え、該通信してよい相手を示す公開鍵と相手プログラム実行・通信装置に付随する公開鍵群の１つ以上の公開鍵とが一致するかどうかを判定することを特徴とする請求項２３または２４記載のプログラムＩＤ通信範囲制御方法。

【請求項２６】　両プログラム実行・通信装置が、相手プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により相手プログラム実行・通信装置の認証を行う工程において、公開鍵によるワン・タイム・パスワード方式が用いられ、自プログラム実行・通信装置は、相手プログラム実行・通信装置から相手プログラム実行・通信装置に付随する公開鍵を得、相手プログラム実行・通信装置にランダムな文字列を送り、相手プログラム実行・通信装置は、該文字列を相手プログラム実行・通信装置に付随する秘密鍵で暗号化して自プログラム実行・通信装置に送り返し、自プログラム実行・通信装置は、暗号化された文字列を相手プログラム実行・通信装置から得た前記公開鍵で復号し、復号した文字列と先に送った文字列とが一致すれば、相手プログラム実行・通信装置を認証することを特徴とする請求項２３または２４記載のプログラムＩＤ通信範囲制御方法。

【請求項２７】　両プログラム実行・通信装置が、相手プログラム実行・通信装置の認証に成功し、かつ両プログラム実行・通信装置による署名確認結果の公開鍵の集まりに一致する公開鍵があるときに、プロセス間の通信路を開く工程において、両プログラム実行・通信装置が、通信路１つあたりに仮想的に複数の仮想通信路を形成する通信装置と、前記プログラムの出所由来を表す公開鍵毎に存在する仮想通信路用資源群と、通信路用資源群とを含み、前記プログラムの出所由来を表す公開鍵が得られた場合に、前記プログラムを元に生成されたプロセスが通信を行う際に、両プログラム実行・通信装置の通信装置が、得られた出所由来を表す公開鍵に対応する仮想通信路資源群の１つに通信路資源を割り当て、仮想通信路資源を使い通信路を提供することを特徴とする請求項２６記載のプログラムＩＤ通信範囲制御方法。

【請求項２８】　プログラムと、各プログラムを元に各プロセスを生成し実行する複数のプログラム実行・通信装置とにより構成される情報システムにおいて、前記プログラム実行・通信装置が、自プログラム実行・通信装置に付随する公開鍵および秘密鍵と、相手プログラム実行・通信装置に付随する公開鍵と、各プログラムを元に生成および実行されるプロセスとを含み、各プログラムが、プログラム本体と、該プログラムの出所由来を表す公開鍵群と、前記プログラム本体および前記公開鍵群を

組み合わせて作成されたデータに対し各公開鍵と対をなす各秘密鍵により行った署名群とを含み、両プログラム実行・通信装置が、各署名が前記プログラム本体および前記公開鍵群を組み合わせて作成されたデータと各署名に対応する各公開鍵と対をなす各秘密鍵とによって生成されたものであるかどうかを確認する工程と、両プログラム実行・通信装置が、相手プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により相手プログラム実行・通信装置の認証を行う工程と、両プログラム実行・通信装置が、自プログラム実行・通信装置による署名確認結果の公開鍵の集まりを相手プログラム実行・通信装置に伝え、自プログラム実行・通信装置による署名確認結果の公開鍵の集まりと相手プログラム実行・通信装置による署名確認結果の公開鍵の集まりとに一致する公開鍵があるかどうかを判定する工程と、相手プログラム実行・通信装置の認証に成功し、かつ両プログラム実行・通信装置による署名確認結果の公開鍵の集まりに一致する公開鍵が１つ以上あるときに、両プログラム実行・通信装置が、プロセス間の通信路を開く工程とを含むことを特徴とするプログラムＩＤ通信範囲制御方法。

【請求項２９】　両プログラム実行・通信装置が、各署名が前記プログラム本体および前記公開鍵群を組み合わせて作成されたデータと各署名に対応する各公開鍵と対をなす各秘密鍵とによって生成されたものであるかどうかを判定する工程において、各署名が前記プログラム本体および前記公開鍵群を組み合わせて作成されたデータをハッシュ関数でハッシングしたダイジェストを前記プログラムの出所由来を表す各公開鍵と対をなす各秘密鍵で暗号化した各署名値からなり、相手プログラム実行・通信装置が、各署名値を前記プログラムの出所由来を表す各公開鍵でそれぞれ復号してダイジェスト群を得るとともに前記プログラム本体および前記公開鍵群で作成されたデータをハッシュ関数でハッシングしてダイジェストを得、該ダイジェストと前記ダイジェスト群とが一致するかどうかを判定することを特徴とする請求項２８記載のプログラムＩＤ通信範囲制御方法。

【請求項３０】　両プログラム実行・通信装置が、相手プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により相手プログラム実行・通信装置の認証を行う工程において、両プログラム実行・通信装置が、通信してよい相手を示す公開鍵を備え、該通信してよい相手を示す公開鍵と相手プログラム実行・通信装置に付随する公開鍵群の１つ以上の公開鍵とが一致するかどうかを判定することを特徴とする請求項２８または２９記載のプログラムＩＤ通信範囲制御方法。

【請求項３１】　両プログラム実行・通信装置が、相手プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により相手プログラム実行・通信装置の認証を行う工程において、公開鍵によるワン・タイム・パスワード方式が用いられ、自プログラム実行・通信装置は、相手プログラム実行・通信装置から相手プログラム実行・通信装置に付随する公開鍵を得、相手プログラム実行・通信装置にランダムな文字列を送り、相手プログラム実行・通信装置は、該文字列を相手プログラム実行・通信装置に付随する秘密鍵で暗号化して自プログラム実行・通信装置に送り返し、自プログラム実行・通信装置は、暗号化された文字列を相手プログラム実行・通信装置から得た前記公開鍵で復号し、復号した文字列と先に送った文字列とが一致すれば、相手プログラム実行・通信装置を認証することを特徴とする請求項２８または２９記載のプログラムＩＤ通信範囲制御方法。

【請求項３２】　両プログラム実行・通信装置が、相手プログラム実行・通信装置の認証に成功し、かつ両プログラム実行・通信装置による署名確認結果の公開鍵の集まりに一致する公開鍵があるときに、プロセス間の通信路を開く工程において、両プログラム実行・通信装置が、通信路１つあたりに仮想的に複数の仮想通信路を形成する通信装置と、前記プログラムの出所由来を表す公開鍵毎に存在する仮想通信路用資源群と、通信路用資源群とを含み、前記プログラムの出所由来を表す公開鍵が１つ以上得られた場合に、前記プログラムを元に生成されたプロセスが通信を行う際に、両プログラム実行・通信装置の通信装置が、得られた出所由来を表す公開鍵に対応する仮想通信路資源群の１つに通信路資源を割り当て、仮想通信路資源を使い通信路を提供することを特徴とする請求項３１記載のプログラムＩＤ通信範囲制御方法。

【請求項３３】　仮想通信路用資源群が仮想的に定義したソケットであり、該仮想通信路資源群の一つ一つが該仮想的に定義したソケットの各ポートに対応し、通信路用資源群が通常のソケットであり、各通信路資源群の一つ一つが該通常のソケット各ポートに対応することを特徴とする請求項２７または３２記載のプログラムＩＤ通信範囲制御方法。

【請求項３４】　プログラムと、該プログラムを元にプロセスを生成し実行および通信するプログラム実行・通信装置とにより構成される情報システムにおいて、前記プログラム実行・通信装置が、前記プログラムを元に生成および実行されるプロセスとを含み、前記プログラムが、プログラム本体と、該プログラムの出所由来を表す公開鍵と、通信路１つあたりに仮想的に複数の仮想通信路を形成する通信装置と、前記プログラムの出所由来を表す公開鍵毎に１つ以上存在する仮想通信路用資源と、１つ以上の通信路用資源とを含み、前記プログラム実行・通信装置が前記プログラムを元に生成されたプロセスの処理により通信を行う際に、出所由来を表す公開鍵と要求された仮想通信路用資源とを対にして仮想通信路と対応させ、仮想通信路を使い通信路を提供する工程をを含むことを特徴とする公開鍵毎通信路提供方法。

【請求項３５】　仮想通信路用資源群が仮想的に定義したソケットであり、該仮想通信路資源群の一つ一つが該仮想的に定義したソケットの各ポートに対応し、通信路用資源群が通常のソケットであり、各通信路資源群の一つ一つが該通常のソケット各ポートに対応することを特徴とする請求項３４記載の公開鍵毎通信路提供方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明はプログラム認証方法，分散環境におけるプログラム間通信により発生する処理のアクセス制御方法，および分散環境におけるプログラムの通信範囲制御方法に関する。

【０００２】

【従来の技術】従来の情報システムの一例は、たとえば図１９に示すように、プログラム本体１０１２１，およびプログラム１０１２の出所由来を表す公開鍵群１０１２２１～１０１２２ｎと秘密鍵群１０１２４１～１０１２４ｎとの対により構成されるプログラム１０１２と、プログラム実行・通信装置である携帯機器１０１によりプログラム１０１２を元に生成および実行されるプロセス１０１２０により構成される、プログラム１０１２を対象としプログラム１０１２を元にプロセス１０１２０を生成し実行する携帯機器１０１と、携帯機器１０１と通信を行う通信・処理装置である親機器１０２とにより、その主要部が構成されていた。

【０００３】従来の情報システムの一例は、たとえば図１９に示すように、プログラム１０１２と、プログラム１０１２を元にプロセス１０１２０を生成し実行するプログラム実行・通信装置である携帯機器１０１と、携帯機器１０１と通信を行う通信・処理装置である親機器１０２とから、その主要部が構成されていた。

【０００４】プログラム１１２は、プログラム本体１０１２１と、プログラム１０１２の出所由来を表す公開鍵群１０１２２１～１０１２２ｎと、公開鍵群１０１２２１～１０１２２ｎと対をなす秘密鍵群１０１２４１～１０１２４ｎとを含んで構成されていた。

【０００５】携帯機器１０１は、組み込み機能部１０１１と、プログラム１０１２を実行するプロセス１０１２０と、携帯機器１０１に付随する公開鍵１０１３２と、公開鍵１０１３２と対をなす秘密鍵１０１３１と、ユーザ・パスワード情報１０１９０とから構成されていた。

【０００６】親機器１０２は、通信してよい相手を表すＩＤである携帯機器１０１に付随する公開鍵１０１３２と、通信してよいユーザを表すユーザ・パスワード情報１０１９０とを含んで構成されていた。

【０００７】このような従来の情報システムでは、プログラム１０１２を元に生成されたプロセス１０１２０の処理により携帯機器１０１が親機器１０２と通信を行う以前に、親機器１０２が、携帯機器１０１から携帯機器１０１に通信をさせるプロセス１０１２０の元となるプログラム１０１２の出所由来を表す公開鍵１０１２２１～１０１２２ｎを得る工程と、親機器１０２が、得られた各公開鍵１０１２２１～１０１２２ｎについて、携帯機器１０１に通信をさせるプロセス１０１２０の元となるプログラム１０１２の出所由来を表す公開鍵群１０１２２１～１０１２２ｎおよび秘密鍵群１０１２４１～１０１２４ｎを用いさせて認証を行うことで、プロセス１０１２０の元となるプログラム１０１２が認証に成功した公開鍵すべてをもつと認証を行っていた。

【０００８】また、従来、情報システムの他の例は、たとえば図２０に示すように、プログラム１０１２と、プログラム１０１２を元にプロセス１０１２０を生成し実行するプログラム実行・通信装置である携帯機器１０１と、携帯機器１０１と通信を行う通信・処理装置である親機器１０２とから、その主要部が構成されていた。

【０００９】携帯機器１０１は、組み込み機能部１０１１と、プログラム１０１２を実行するプロセス１０１２０と、携帯機器１０１に付随する公開鍵１０１３２および秘密鍵１０１３１と、ユーザ・パスワード情報１０１９０とから構成されていた。

【００１０】親機器１０２は、通信してよい相手を示す公開鍵としての携帯機器１０１に付随する公開鍵１０１３２と、ユーザ・パスワード情報１０１９０とをもつ。

【００１１】このような従来の情報システムでは、携帯機器１０１で、ユーザ・パスワード情報１０１９０について認証を行い、プログラム１０１２を実行するプロセス１０１２０がユーザ・パスワード情報１０１９０を保持する。プロセス１０１２０が親機器１０２と通信をしようとして通信要求が発生した場合、親機器１０２は、携帯機器１０１から公開鍵１０１３２を受け取り、公開鍵１０１３２と一致するものであれば、携帯機器１０１に対し公開鍵１０１３２について認証を行い、認証に成功した場合は、携帯機器１０１内のプログラム１０１２を実行するプロセス１０１２０と親機器１０２との通信を許し、またその通信によって発生する処理についてのアクセス制御は、通信相手によらず同じアクセス制御を行うか、または通信相手のプロセス１０１２０のもつユーザ・パスワード情報１０１９０を引き継ぎ、ユーザ認証が成功すればそれをもとにアクセス制御を行っていた。

【００１２】さらに、従来、情報システムの別の例は、たとえば図２１に示すように、携帯機器１０１と、親機器１０２とから、その主要部が構成されていた。

【００１３】携帯機器１０１は、組み込み機能部１０１１と、プログラム１０１２と、プログラム１０１２を実行するプロセス１０１２０と、携帯機器１０１に付随する秘密鍵１０１３１と、秘密鍵１０１３１と対をなす公開鍵１０１３２と、通信してよい相手を示す公開鍵１０２３２とを含んで構成されていた。

【００１４】親機器１０２は、組み込み機能部１０２１

と、プログラム１０２２と、プログラム１０２２を実行するプロセス１０２２０と、親機器１０２に付随する秘密鍵１０２３１と、秘密鍵１０２３１と対を成す公開鍵１０２３２と、通信してよい相手を示す公開鍵１０１３２とから構成されていた。

【００１５】このような従来の情報システムでは、プロセス１０１２０とプロセス１０２２０とが通信をしようとして通信要求が発生した場合、組み込み機能部１０１１および１０２１は、まず、公開鍵１０１３２および１０２３２を互いに渡し、受け取った公開鍵１０２３２および１０１３２と通信してよい相手を示す公開鍵１０２３２および１０１０３２とをそれぞれ比較する。一致すれば、各組み込み機能部１０１１および１０２１は、受け取った公開鍵１０２３２および１０１３２で相互認証を行い、相互認証が成功すれば、プロセス１０１２０とプロセス１０２２０との通信を許す。一方、受け取った公開鍵１０２３２および１０１３２と通信してよい相手を示す公開鍵１０１３３および１０２３３とが異なるか、公開鍵１０２３２および１０１３２での相互認証が失敗した場合は、プロセス１０１２０とプロセス１０２２０との間の通信を許さなかった。また通信路資源群を仮想的に公開鍵毎に別資源として提供していなかった。

【００１６】

【発明が解決しようとする課題】第１の問題点は、通信時の成りすましを防ぐためには、プログラムが存在するエリア（メモリ，ディスク等）のセキュリティレベルとして、読み出し改竄不可でなければならないということである。その理由は、プログラムが秘密鍵をもつ必要があるからである。

【００１７】第２の問題点は、分散環境において、ユーザ・パスワード情報に類する共通の情報を保持し、維持管理する必要があることである。その理由は、認証するために同じユーザ・パスワード情報に類する情報を共有する必要があるからである。

【００１８】第３の問題点は、ユーザ・パスワード情報に類する情報を利用しない場合は、通信相手によらず皆同じ権限で処理を実行させることである。その理由は、アクセス制御をするための正当性を保証できる情報を得られないからである。

【００１９】第４の問題点は、機器，プログラムないしはシステムの設計時に機器，プログラムないしはプロセスの通信すべき相手をどのプログラムとするかを個別に設計しなければならないということである。その理由は、通信相手は通信すべき相手がもつているはずの公開鍵の設定によって決まるからである。

【００２０】第５の問題点は、システムの拡張および複数のシステムの乗り入れの際の手間が多いということである。その理由は、システムの拡張および複数のシステムの乗り入れのための、機器，プログラムないしはシステムの設計時に機器，プログラムないしはプロセスの通信すべき相手をどのプログラムとするかを個々に設計し直さなければならないからである。

【００２１】第６の問題点は、システムが特定のサービスに固定したものになりがちであることである。その理由は、システムの拡張および複数のシステムの乗り入れの際の手間が多いからである。

【００２２】第７の問題点は、どの通信路をどの公開鍵に対応し利用するか設計、管理する必要があることである。その理由は、通信路資源群を仮想的に公開鍵毎に別資源として提供していなかったからである。

【００２３】本発明の第１の目的は、プログラムが存在するエリアのセキュリティレベルとして、読み出し改竄可でよい環境での、通信における成りすましを防止する秘密鍵なしプログラム認証方法を提供することにある。

【００２４】本発明の第２の目的は、集中管理下にない分散環境におけるプログラム間通信により発生する処理のアクセス制御を行うためのプログラムＩＤ通信処理制御方法を提供することにある。

【００２５】本発明の第３の目的は、分散環境において、通信の範囲、つまり情報の流通について範囲が予め限定されており、通信範囲に関するシステム設計が容易なプログラムＩＤ通信範囲制御方法を提供することにある。

【００２６】本発明の第４の目的は、公開鍵別の通信を行う場合に、どの通信路がどの公開鍵用で占有されるかが予め限定されており、通信路に関するシステム設計が容易な公開鍵毎通信路提供方法を提供することにある。

【００２７】なお、先行技術文献として特開２０００－１４８４６９があるが、この公報に開示された「モジュラーアプリケーション間のサービスへのアクセス制御」方法は、第１のコンピュータプログラムモジュールが第２のコンピュータプログラムモジュールからサービスのアクセスを与える権力をデジタル的に署名されたかどうかを判定し、デジタル的に署名された場合に第１のコンピュータプログラムモジュールにサービスへのアクセスを提供するようにしたものである。しかし、この方法は、第１のコンピュータプログラムモジュールが第２のコンピュータプログラムモジュールからのサービスにアクセスできるように、第１のコンピュータプログラムモジュールおよび第２のコンピュータプログラムモジュールを同じコンピューティングノード上の同じアドレス空間内で実行させることができるようにするためのものであり、本発明のように異なるプログラム実行・通信装置上で異なるプログラムを通信を介して協働させるようにするためのものではない。

【００２８】

【課題を解決するための手段】本発明の秘密鍵なしプログラム認証方法は、プログラムと、該プログラムを元にプロセスを生成し実行するプログラム実行・通信装置と、該プログラム実行・通信装置と通信を行う通信・処

理装置とにより構成される情報システムにおいて、前記プログラム実行・通信装置が、該プログラム実行・通信装置に付随する公開鍵および秘密鍵と、前記プログラムを元に生成および実行されるプロセスとを含み、前記プログラムが、プログラム本体と、該プログラムの出所由来を表す公開鍵と、前記プログラム本体に対し該公開鍵と対をなす秘密鍵により行った署名とを含み、前記プログラム実行・通信装置が、前記署名が前記プログラム本体と前記プログラムの出所由来を表す公開鍵と対をなす秘密鍵とによって生成されたものであるかどうかを確認する工程と、前記プログラム実行・通信装置が前記プログラムを元に生成されたプロセスの処理により前記通信・処理装置と通信を行う以前に、前記通信・処理装置が、前記プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により前記プログラム実行・通信装置の認証を行う工程と、前記署名が前記プログラム本体と前記プログラムの出所由来を表す公開鍵と対をなす秘密鍵とによって生成されたものであることが確認できた場合に、前記プログラム実行・通信装置が前記プログラムを元に生成されたプロセスの処理により前記通信・処理装置と通信を行う以前に、前記通信・処理装置が前記プログラムの出所由来を表す公開鍵を得る工程と、前記プログラム実行・通信装置の認証に成功し、かつ前記プログラムの出所由来を表す公開鍵を得られた場合に、前記通信・処理装置が該公開鍵を前記プログラムの出所由来を表すと認証する工程とを含むことを特徴とする。

【００２９】また、本発明の秘密鍵なしプログラム認証方法は、前記プログラム実行・通信装置が、前記署名が前記プログラム本体と前記プログラムの出所由来を表す公開鍵と対をなす秘密鍵とによって生成されたものであるかどうかを確認する工程において、前記署名が前記プログラム本体をハッシュ関数でハッシングしたダイジェストを前記プログラムの出所由来を表す公開鍵と対をなす秘密鍵で暗号化した署名値からなり、前記プログラム実行・通信装置が、前記署名値を前記プログラムの出所由来を表す公開鍵で復号してダイジェストを得るとともに前記プログラム本体をハッシュ関数でハッシングしてダイジェストを得、両ダイジェストが一致するかどうかを判定することを特徴とする。

【００３０】さらに、本発明の秘密鍵なしプログラム認証方法は、前記通信・処理装置が、前記プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により前記プログラム実行・通信装置の認証を行う工程において、前記通信・処理装置が、通信してよい相手を示す公開鍵を備え、該通信してよい相手を示す公開鍵と前記プログラム実行・通信装置に付随する公開鍵とが一致するかどうかを判定し、一致する場合に前記プログラム実行・通信装置を認証することを特徴とする。

【００３１】さらにまた、本発明の秘密鍵なしプログラム認証方法は、前記通信・処理装置が、前記プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により前記プログラム実行・通信装置の認証を行う工程において、公開鍵によるワン・タイム・パスワード方式が用いられ、前記通信・処理装置は、前記プログラム実行・通信装置にランダムな文字列を送り、前記プログラム実行・通信装置は、該文字列を該プログラム実行・通信装置に付随する秘密鍵で暗号化して前記通信・処理装置に送り返し、前記通信・処理装置は、暗号化された文字列を事前に保持する通信してよい相手を示す公開鍵で復号し、復号した文字列と先に送った文字列とが一致すれば、前記プログラム実行・通信装置を認証することを特徴とする。

【００３２】また、本発明の秘密鍵なしプログラム認証方法は、プログラムと、該プログラムを元にプロセスを生成し実行するプログラム実行・通信装置と、該プログラム実行・通信装置と通信を行う通信・処理装置とにより構成される情報システムにおいて、前記プログラム実行・通信装置が、該プログラム実行・通信装置に付随する公開鍵および秘密鍵と、前記プログラムを元に生成および実行されるプロセスとを含み、前記プログラムが、プログラム本体と、該プログラムの出所由来を表す公開鍵群と、前記プログラム本体および前記公開鍵群を組み合わせて作成されたデータに対し各公開鍵と対をなす各秘密鍵により行った署名群とを含み、前記プログラム実行・通信装置が、各署名が前記プログラム本体および前記公開鍵群を組み合わせて作成されたデータと各署名に対応する各公開鍵と対をなす各秘密鍵とによって生成されたものであるかどうかを確認し、生成されたものであることが確認された署名に対応する公開鍵の集まりを得る工程と、前記プログラム実行・通信装置が前記プログラムを元に生成されたプロセスの処理により前記通信・処理装置と通信を行う以前に、前記通信・処理装置が、前記プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により前記プログラム実行・通信装置の認証を行う工程と、前記生成されたものであることが確認された署名に対応する公開鍵が１つ以上得られた場合に、前記プログラム実行・通信装置が前記プログラムを元に生成されたプロセスの処理により前記通信・処理装置と通信を行う以前に、前記通信・処理装置が前記プログラムの出所由来を表す公開鍵を得る工程と、前記プログラム実行・通信装置の認証に成功し、かつ前記プログラムの出所由来を表す公開鍵を得られた場合に、前記通信・処理装置が、前記プログラム実行・通信装置による署名確認結果の各公開鍵を、前記プログラムの出所由来を表すと認証する工程とを含むことを特徴とする。

【００３３】さらに、本発明の秘密鍵なしプログラム認証方法は、前記プログラム実行・通信装置が、各署名が前記プログラム本体および前記公開鍵群を組み合わせて

作成されたデータと各署名に対応する各公開鍵と対をなす各秘密鍵とによって生成されたものであるかどうかを確認し、確認した署名に対応する公開鍵の集まりを得る工程において、各署名が前記プログラム本体および前記公開鍵群の組み合わせで作成されたデータをハッシュ関数でハッシングしたダイジェストを前記プログラムの出所由来を表す各公開鍵と対をなす各秘密鍵で暗号化した各署名値からなり、前記プログラム実行・通信装置が、各署名値を前記プログラムの出所由来を表す各公開鍵でそれぞれ復号してダイジェスト群を得るとともに前記プログラム本体および前記公開鍵群の組み合わせで作成されたデータをハッシュ関数でハッシングしてダイジェストを得、該ダイジェストと前記ダイジェスト群とが一致するかどうかを判定することを特徴とする。

【００３４】さらにまた、本発明の秘密鍵なしプログラム認証方法は、前記通信・処理装置が、前記プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により前記プログラム実行・通信装置の認証を行う工程において、前記通信・処理装置が、通信してよい相手を示す公開鍵を備え、該通信してよい相手を示す公開鍵と前記プログラム実行・通信装置に付随する公開鍵とが一致するかどうかを判定し、一致する場合に前記プログラム実行・通信装置を認証することを特徴とする。

【００３５】また、本発明の秘密鍵なしプログラム認証方法は、前記通信・処理装置が、前記プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により前記プログラム実行・通信装置の認証を行う工程において、公開鍵によるワン・タイム・パスワード方式が用いられ、前記通信・処理装置は、前記プログラム実行・通信装置にランダムな文字列を送り、前記プログラム実行・通信装置は、該文字列を該プログラム実行・通信装置に付随する秘密鍵で暗号化して前記通信・処理装置に送り返し、前記通信・処理装置は、暗号化された文字列を事前に保持する通信してよい相手を示す公開鍵で復号し、復号した文字列と先に送った文字列とが一致すれば、前記プログラム実行・通信装置を認証することを特徴とする。

【００３６】一方、本発明のプログラムＩＤ通信処理制御方は、プログラムと、該プログラムを元にプロセスを生成し実行するプログラム実行・通信装置と、該プログラム実行・通信装置と通信を行う通信・処理装置とにより構成される情報システムにおいて、前記プログラムが、プログラム本体と、該プログラムの出所由来を表すＩＤ群とを含み、前記プログラム実行・通信装置が、前記プログラムを元に生成および実行されるプロセスを含み、前記プログラム実行・通信装置が前記プログラムを元に生成されたプロセスの処理により前記通信・処理装置と通信を行う以前に、前記通信・処理装置が、前記プロセスの元となるプログラムの出所由来を表すＩＤ群の一部または全部を得る工程と、前記出所由来を表すＩＤが１つ以上得られたときに、前記通信・処理装置が前記プログラムを元に生成されたプロセスの処理により前記プログラム実行・通信装置と通信を行う工程と、通信によって発生した処理において、前記通信・処理装置が、前記プログラム実行・管理装置から得られた前記出所由来を表すＩＤ群を元にしたアクセス制御を行う工程とを含むことを特徴とする。

【００３７】また、本発明のプログラムＩＤ通信処理制御方法は、プログラムと、該プログラムを元にプロセスを生成し実行するプログラム実行・通信装置と、該プログラム実行・通信装置と通信を行う通信・処理装置とにより構成される情報システムにおいて、前記プログラムが、プログラム本体，該プログラムの出所由来を表す公開鍵，および該公開鍵と対をなす秘密鍵を含み、前記プログラム実行・通信装置が、前記プログラムを元に生成および実行されるプロセスを含み、前記プログラム実行・通信装置が前記プログラムを元に生成されたプロセスの処理により前記通信・処理装置と通信を行う以前に、前記通信・処理装置が、前記プログラム実行・通信装置から該プログラム実行・通信装置に通信をさせるプロセスの元となる前記プログラムの出所由来を表す公開鍵を得る工程と、前記通信・処理装置が、前記プログラムの出所由来を表す公開鍵および秘密鍵を用いた公開鍵方式により前記プログラムの認証を行う工程と、前記プログラムが認証されたときに、前記通信・処理装置が、前記公開鍵を元にしたアクセス制御により前記プログラム実行・通信装置と通信を行う工程とを含むことを特徴とする。

【００３８】さらに、本発明のプログラムＩＤ通信処理制御方法は、前記通信・処理装置が、得られた公開鍵について、前記プログラムの出所由来を表す公開鍵および秘密鍵を用いた公開鍵方式により前記プログラムの認証を行う工程において、公開鍵によるワン・タイム・パスワード方式が用いられ、前記プログラム実行・通信装置が、前記公開鍵を前記通信・処理装置に送り、前記通信・処理装置が、前記プログラム実行・通信装置にランダムな文字列を送り、前記プログラム実行・通信装置が、該文字列を前記秘密鍵で暗号化した文字列を前記通信・処理装置に送り返し、前記通信・処理装置が、暗号化された文字列を前記送られてきた公開鍵で復号し、復号した文字列と先に送った文字列とが一致すれば、前記プログラムを認証することを特徴とする。

【００３９】さらにまた、本発明のプログラムＩＤ通信処理制御方法は、プログラムと、該プログラムを元にプロセスを生成し実行するプログラム実行・通信装置と、該プログラム実行・通信装置と通信を行う通信・処理装置とにより構成される情報システムにおいて、前記プログラム実行・通信装置が、該プログラム実行・通信装置に付随する公開鍵および秘密鍵と、前記プログラムを元

に生成および実行されるプロセスとを含み、前記プログラムが、プログラム本体と、該プログラムの出所由来を表す公開鍵と、前記プログラム本体に対し該公開鍵と対をなす秘密鍵により行った署名とを含み、前記プログラム実行・通信装置が、前記署名が前記プログラム本体と前記プログラムの出所由来を表す公開鍵と対をなす秘密鍵とによって生成されたものであるかどうかを確認する工程と、前記プログラム実行・通信装置が前記プログラムを元に生成されたプロセスの処理により前記通信・処理装置と通信を行う以前に、前記通信・処理装置が、前記プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により前記プログラム実行・通信装置の認証を行う工程と、前記署名が前記プログラム本体と前記プログラムの出所由来を表す公開鍵と対をなす秘密鍵とによって生成されたものであることが確認できた場合に、前記プログラム実行・通信装置が前記プログラムを元に生成されたプロセスの処理により前記通信・処理装置と通信を行う以前に、前記通信・処理装置が前記プログラムの出所由来を表す公開鍵を得る工程と、前記プログラム実行・通信装置の認証に成功し、かつ前記プログラムの出所由来を表す公開鍵を得られた場合に、前記通信・処理装置が、前記プログラム実行・通信装置から前記プログラムの出所由来を表す公開鍵を得、該公開鍵を元にしたアクセス制御により前記プログラム実行・通信装置と通信を行う工程とを含むことを特徴とする。

【００４０】また、本発明のプログラムＩＤ通信処理制御方法は、前記プログラム実行・通信装置が、前記署名が前記プログラム本体と前記プログラムの出所由来を表す公開鍵と対をなす秘密鍵とによって生成されたものであるかどうかを確認する工程において、前記署名が前記プログラム本体をハッシュ関数でハッシングしたダイジェストを前記プログラムの出所由来を表す公開鍵と対をなす秘密鍵で暗号化した署名値からなり、前記プログラム実行・通信装置が、前記署名値を前記プログラムの出所由来を表す公開鍵で復号してダイジェストを得るとともに前記プログラム本体をハッシュ関数でハッシングしてダイジェストを得、両ダイジェストが一致するかどうかを判定することを特徴とする。

【００４１】さらに、本発明のプログラムＩＤ通信処理制御方法は、前記通信・処理装置が、前記プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により前記プログラム実行・通信装置の認証を行う工程において、前記通信・処理装置が、通信してよい相手を示す公開鍵を備え、前記プログラム実行・通信装置に付随する公開鍵と前記通信してよい相手を示す公開鍵とが一致するかどうかを判定することを特徴とする。

【００４２】さらにまた、本発明のプログラムＩＤ通信処理制御方法は、前記通信・処理装置が、前記プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により前記プログラム実行・通信装置の認証を行う工程において、公開鍵によるワン・タイム・パスワード方式が用いられ、前記通信・処理装置は、前記プログラム実行・通信装置にランダムな文字列を送り、前記プログラム実行・通信装置は、該文字列を該プログラム実行・通信装置に付随する秘密鍵で暗号化して前記通信・処理装置に送り返し、前記通信・処理装置は、暗号化された文字列を事前に保持する通信してよい相手を示す公開鍵で復号し、復号した文字列と先に送った文字列とが一致すれば、前記プログラム実行・通信装置を認証することを特徴とする。

【００４３】また、本発明のプログラムＩＤ通信処理制御方法は、プログラムと、該プログラムを元にプロセスを生成し実行するプログラム実行・通信装置と、該プログラム実行・通信装置と通信を行う通信・処理装置とにより構成される情報システムにおいて、前記プログラム実行・通信装置が、該プログラム実行・通信装置に付随する公開鍵および秘密鍵と、前記プログラムを元に生成および実行されるプロセスとを含み、前記プログラムが、プログラム本体と、該プログラムの出所由来を表す公開鍵群と、前記プログラム本体および前記公開鍵群を組み合わせて作成されたデータに対し各公開鍵と対をなす各秘密鍵により行った署名群とを含み、前記プログラム実行・通信装置が、各署名が前記プログラム本体および前記公開鍵群を組み合わせて作成されたデータと各署名に対応する各公開鍵と対をなす各秘密鍵とによって生成されたものであるかどうかを確認し、生成されたものであることが確認された署名に対応する公開鍵の集まりを得る工程と、前記プログラム実行・通信装置が前記プログラムを元に生成されたプロセスの処理により前記通信・処理装置と通信を行う以前に、前記通信・処理装置が、前記プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により前記プログラム実行・通信装置の認証を行う工程と、前記生成されたものであることが確認された署名に対応する公開鍵が１つ以上得られた場合に、前記プログラム実行・通信装置が前記プログラムを元に生成されたプロセスの処理により前記通信・処理装置と通信を行う以前に、前記通信・処理装置が前記プログラムの出所由来を表す公開鍵を得る工程と、前記プログラム実行・通信装置の認証に成功し、かつ前記プログラムの出所由来を表す公開鍵を得られた場合に、前記通信・処理装置が、前記プログラム実行・通信装置による署名確認結果の公開鍵の集まりの一部または全部を元にしたアクセス制御により前記プログラム実行・通信装置と通信を行う工程とを含むことを特徴とする。

【００４４】さらに、本発明のプログラムＩＤ通信処理制御方法は、前記プログラム実行・通信装置が、各署名が前記プログラム本体および前記公開鍵群を組み合わせ

て作成されたデータと各署名に対応する各公開鍵と対をなす各秘密鍵とによって生成されたものであるかどうかを確認する工程において、各署名が前記プログラム本体および前記公開鍵群を組み合わせて作成されたデータをハッシュ関数でハッシングしたダイジェストを前記プログラムの出所由来を表す各公開鍵と対をなす各秘密鍵で暗号化した各署名値からなり、前記プログラム実行・通信装置が、各署名値を各公開鍵でそれぞれ復号した各ダイジェストと、前記プログラム本体および前記公開鍵群を組み合わせて作成されたデータをハッシュ関数でハッシングして得られるダイジェストとが一致するかどうかを判定することを特徴とする。

【００４５】さらにまた、本発明のプログラムＩＤ通信処理制御方法は、前記通信・処理装置が、前記プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により前記プログラム実行・通信装置の認証を行う工程において、前記通信・処理装置が、通信してよい相手を示す公開鍵を備え、前記プログラム実行・通信装置に付随する公開鍵と前記通信してよい相手を示す公開鍵とが一致するかどうかを判定することを特徴とする。

【００４６】また、本発明のプログラムＩＤ通信処理制御方法は、前記通信・処理装置が、前記プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により前記プログラム実行・通信装置の認証を行う工程において、公開鍵によるワン・タイム・パスワード方式が用いられ、前記通信・処理装置は、前記プログラム実行・通信装置にランダムな文字列を送り、前記プログラム実行・通信装置は、該文字列を該プログラム実行・通信装置に付随する秘密鍵で暗号化して前記通信・処理装置に送り返し、前記通信・処理装置は、暗号化された文字列を事前に保持する通信してよい相手を示す公開鍵で復号し、復号した文字列と先に送った文字列とが一致すれば、前記プログラム実行・通信装置を認証することを特徴とする。

【００４７】他方、本発明のプログラムＩＤ通信範囲制御方法は、プログラムと、これらプログラムを元にプロセスをそれぞれ生成し実行する複数のプログラム実行・通信装置とにより構成される情報システムにおいて、前記プログラムが、プログラム本体，および該プログラムの出所由来を表すＩＤ群を含み、あるプログラムを元にあるプログラム実行・通信装置が生成したあるプロセスが、該プログラムまたは別のあるプログラムを元に別のあるプログラム実行・通信装置が生成した別のあるプロセスと通信を行う前に、両プログラム実行・通信装置が、相手プログラム実行・通信装置内のプロセスの元となる前記プログラムの出所由来を表すＩＤ群の一部または全部を得る工程と、前記出所由来を表すＩＤ群が得られたときに、両プログラム実行・通信装置が、得られた出所由来を表すＩＤ群と自プログラム実行・通信装置内のプロセスの元となる前記プログラムの出所由来を表すＩＤ群とを比較し、一致する前記プログラムの出所由来を表すＩＤが１つ以上存在すれば通信路を開く工程とを含むことを特徴とする。

【００４８】また、本発明のプログラムＩＤ通信範囲制御方法は、プログラムと、各プログラムを元に各プロセスを生成し実行する複数のプログラム実行・通信装置とにより構成される情報システムにおいて、前記プログラムが、プログラム本体，該プログラムの出所由来を表す公開鍵，および該公開鍵と対をなす秘密鍵を含み、あるプログラムを元にあるプログラム実行・通信装置が生成したあるプロセスが、該プログラムまたは別のあるプログラムを元に別のあるプログラム実行・通信装置が生成した別のあるプロセスと通信を行う前に、両プログラム実行・通信装置が、相手プログラム実行・通信装置から相手プログラム実行・通信装置内のプロセスの元となる前記プログラムの出所由来を表す公開鍵をそれぞれ得る工程と、両プログラム実行・通信装置が、相手プログラム実行・通信装置から得られた公開鍵と自プログラム実行・通信装置内のプロセスの元となる前記プログラムの出所由来を表す公開鍵とが一致するかどうかを判定する工程と、両プログラム実行・通信装置が、相手プログラム実行・通信装置内のプロセスの元となる前記プログラムの出所由来を表す公開鍵および秘密鍵を用いて相手プログラム実行・通信装置内のプロセスの元となるプログラムの相互認証を行う工程と、相手プログラム実行・通信装置から得られた公開鍵と自プログラム実行・通信装置内のプロセスの元となる前記プログラムの出所由来を表す公開鍵とが一致し、かつ相手プログラム実行・通信装置内のプロセスの元となるプログラムが相互認証されたときに、両プログラム実行・通信装置が通信路を開く工程とを含むことを特徴とする。

【００４９】また、本発明のプログラムＩＤ通信範囲制御方法は、両プログラム実行・通信装置が、相手プログラム実行・通信装置内のプロセスの元となる前記プログラムの出所由来を表す公開鍵および秘密鍵を用いて相手プログラム実行・通信装置内のプロセスの元となるプログラムの相互認証を行う工程において、公開鍵によるワン・タイム・パスワード方式が用いられ、両プログラム実行・通信装置が、自プログラム実行・通信装置に付随する公開鍵を相手プログラム実行・通信装置に送り、相手プログラム実行・通信装置にランダムな文字列をそれぞれ送り、相手プログラム実行・通信装置が、該文字列を相手プログラム実行・通信装置内のプロセスの元となる前記プログラムの出所由来を表す公開鍵と対をなす秘密鍵で暗号化した文字列を自プログラム実行・通信装置に送り返し、自プログラム実行・通信装置が、暗号化された文字列を対応する公開鍵で復号し、復号した文字列と先に送った文字列とが一致すれば、相手プログラム実行・通信装置通信装置内のプロセスの元となるプログラ

ムを認証することを特徴とする。

【００５０】さらに、本発明のプログラムＩＤ通信範囲制御方法は、プログラムと、各プログラムを元に各プロセスを生成し実行する複数のプログラム実行・通信装置とにより構成される情報システムにおいて、前記プログラム実行・通信装置が、自プログラム実行・通信装置に付随する公開鍵および秘密鍵と、相手プログラム実行・通信装置に付随する公開鍵と、前記プログラムを元に生成および実行されるプロセスとを含み、前記プログラムが、プログラム本体と、該プログラムの出所由来を表す公開鍵と、前記プログラム本体に対し該公開鍵と対をなす秘密鍵により行った署名とを含み、あるプログラムを元にあるプログラム実行・通信装置が生成したあるプロセスが、該プログラムまたは別のあるプログラムを元に別のあるプログラム実行・通信装置が生成した別のあるプロセスと通信を行う前に、両プログラム実行・通信装置が、前記署名が前記プログラム本体と前記前記プログラムの出所由来を表す公開鍵と対をなす秘密鍵とによって生成されたものであるかどうかを確認する工程と、前記通信を行う前に、両プログラム実行・通信装置が、相手プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により相手プログラム実行・通信装置の認証を行う工程と、両プログラム実行・通信装置が、前記署名が前記プログラム本体と前記プログラムの出所由来を表す公開鍵と対をなす秘密鍵とによって生成されたものであることが確認できた場合に、前記通信を行う前に、前記公開鍵を相手プログラム実行・通信装置に伝える工程と、両プログラム実行・通信装置が、相手プログラム実行・通信装置から得られた公開鍵と自プログラム実行・通信装置内のプロセスの元となる前記プログラムの出所由来を表す公開鍵とが一致するかどうかを判定する工程と、相手プログラム実行・通信装置内のプロセスの元となるプログラムが相互認証され、かつ相手プログラム実行・通信装置から得られた公開鍵と自プログラム実行・通信装置内のプロセスの元となる前記プログラムの出所由来を表す公開鍵とが一致したときに、両プログラム実行・通信装置が通信路を開く工程とを含むことを特徴とする。

【００５１】さらにまた、本発明のプログラムＩＤ通信範囲制御方法は、両プログラム実行・通信装置が、前記署名が前記プログラム本体と前記プログラムの出所由来を表す公開鍵と対をなす秘密鍵とによって生成されたものであるかどうかを確認する工程において、前記署名が前記プログラム本体をハッシュ関数でハッシングしたダイジェストを前記プログラムの出所由来を表す公開鍵と対をなす秘密鍵で暗号化した署名値からなり、両プログラム実行・通信装置が、前記署名値を前記プログラムの出所由来を表す公開鍵で復号してダイジェストを得るとともに前記プログラム本体をハッシュ関数でハッシングしてダイジェストを得、両ダイジェストが一致するかどうかを判定することを特徴とする。

【００５２】また、本発明のプログラムＩＤ通信範囲制御方法は、両プログラム実行・通信装置が、相手プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により相手プログラム実行・通信装置の認証を行う工程において、両プログラム実行・通信装置が、通信してよい相手を示す公開鍵を備え、該通信してよい相手を示す公開鍵と相手プログラム実行・通信装置に付随する公開鍵群の１つ以上の公開鍵とが一致するかどうかを判定することを特徴とする。

【００５３】さらに、本発明のプログラムＩＤ通信範囲制御方法は、両プログラム実行・通信装置が、相手プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により相手プログラム実行・通信装置の認証を行う工程において、公開鍵によるワン・タイム・パスワード方式が用いられ、自プログラム実行・通信装置は、相手プログラム実行・通信装置から相手プログラム実行・通信装置に付随する公開鍵を得、相手プログラム実行・通信装置にランダムな文字列を送り、相手プログラム実行・通信装置は、該文字列を相手プログラム実行・通信装置に付随する秘密鍵で暗号化して自プログラム実行・通信装置に送り返し、自プログラム実行・通信装置は、暗号化された文字列を相手プログラム実行・通信装置から得た前記公開鍵で復号し、復号した文字列と先に送った文字列とが一致すれば、相手プログラム実行・通信装置を認証することを特徴とする。

【００５４】さらにまた、本発明のプログラムＩＤ通信範囲制御方法は、両プログラム実行・通信装置が、相手プログラム実行・通信装置の認証に成功し、かつ両プログラム実行・通信装置による署名確認結果の公開鍵の集まりに一致する公開鍵があるときに、プロセス間の通信路を開く工程において、両プログラム実行・通信装置が、通信路１つあたりに仮想的に複数の仮想通信路を形成する通信装置と、前記プログラムの出所由来を表す公開鍵毎に存在する仮想通信路用資源群と、通信路用資源群とを含み、前記プログラムの出所由来を表す公開鍵が得られた場合に、前記プログラムを元に生成されたプロセスが通信を行う際に、両プログラム実行・通信装置の通信装置が、得られた出所由来を表す公開鍵に対応する仮想通信路資源群の１つに通信路資源を割り当て、仮想通信路資源を使い通信路を提供することを特徴とする。

【００５５】また、本発明のプログラムＩＤ通信範囲制御方法は、プログラムと、各プログラムを元に各プロセスを生成し実行する複数のプログラム実行・通信装置とにより構成される情報システムにおいて、前記プログラム実行・通信装置が、自プログラム実行・通信装置に付随する公開鍵および秘密鍵と、相手プログラム実行・通信装置に付随する公開鍵と、各プログラムを元に生成および実行されるプロセスとを含み、各プログラムが、プログラム本体と、該プログラムの出所由来を表す公開鍵

群と、前記プログラム本体および前記公開鍵群を組み合わせて作成されたデータに対し各公開鍵と対をなす各秘密鍵により行った署名群とを含み、両プログラム実行・通信装置が、各署名が前記プログラム本体および前記公開鍵群を組み合わせて作成されたデータと各署名に対応する各公開鍵と対をなす各秘密鍵とによって生成されたものであるかどうかを確認する工程と、両プログラム実行・通信装置が、相手プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により相手プログラム実行・通信装置の認証を行う工程と、両プログラム実行・通信装置が、自プログラム実行・通信装置による署名確認結果の公開鍵の集まりを相手プログラム実行・通信装置に伝え、自プログラム実行・通信装置による署名確認結果の公開鍵の集まりと相手プログラム実行・通信装置による署名確認結果の公開鍵の集まりとに一致する公開鍵があるかどうかを判定する工程と、相手プログラム実行・通信装置の認証に成功し、かつ両プログラム実行・通信装置による署名確認結果の公開鍵の集まりに一致する公開鍵が1つ以上あるときに、両プログラム実行・通信装置が、プロセス間の通信路を開く工程とを含むことを特徴とする。

【0056】さらに、本発明のプログラムID通信範囲制御方法は、両プログラム実行・通信装置が、各署名が前記プログラム本体および前記公開鍵群を組み合わせて作成されたデータと各署名に対応する各公開鍵と対をなす各秘密鍵とによって生成されたものであるかどうかを判定する工程において、各署名が前記プログラム本体および前記公開鍵群を組み合わせて作成されたデータをハッシュ関数でハッシングしたダイジェストを前記プログラムの出所由来を表す各公開鍵と対をなす各秘密鍵で暗号化した各署名値からなり、相手プログラム実行・通信装置が、各署名値を前記プログラムの出所由来を表す各公開鍵でそれぞれ復号してダイジェスト群を得るとともに前記プログラム本体および前記公開鍵群で作成されたデータをハッシュ関数でハッシングしてダイジェストを得、該ダイジェストと前記ダイジェスト群とが一致するかどうかを判定することを特徴とする。

【0057】さらにまた、本発明のプログラムID通信範囲制御方法は、両プログラム実行・通信装置が、相手プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により相手プログラム実行・通信装置の認証を行う工程において、両プログラム実行・通信装置が、通信してよい相手を示す公開鍵を備え、該通信してよい相手を示す公開鍵と相手プログラム実行・通信装置に付随する公開鍵群の1つ以上の公開鍵とが一致するかどうかを判定することを特徴とする。

【0058】また、本発明のプログラムID通信範囲制御方法は、両プログラム実行・通信装置が、相手プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により相手プログラム実行・通信装置の認証を行う工程において、公開鍵によるワン・タイム・パスワード方式が用いられ、自プログラム実行・通信装置は、相手プログラム実行・通信装置から相手プログラム実行・通信装置に付随する公開鍵を得、相手プログラム実行・通信装置にランダムな文字列を送り、相手プログラム実行・通信装置は、該文字列を相手プログラム実行・通信装置に付随する秘密鍵で暗号化して自プログラム実行・通信装置に送り返し、自プログラム実行・通信装置は、暗号化された文字列を相手プログラム実行・通信装置から得た前記公開鍵で復号し、復号した文字列と先に送った文字列とが一致すれば、相手プログラム実行・通信装置を認証することを特徴とする。

【0059】さらに、本発明のプログラムID通信範囲制御方法は、両プログラム実行・通信装置が、相手プログラム実行・通信装置の認証に成功し、かつ両プログラム実行・通信装置による署名確認結果の公開鍵の集まりに一致する公開鍵があるときに、プロセス間の通信路を開く工程において、両プログラム実行・通信装置が、通信路1つあたりに仮想的に複数の仮想通信路を形成する通信装置と、前記プログラムの出所由来を表す公開鍵毎に存在する仮想通信路用資源群と、通信路用資源群とを含み、前記プログラムの出所由来を表す公開鍵が1つ以上得られた場合に、前記プログラムを元に生成されたプロセスが通信を行う際に、両プログラム実行・通信装置の通信装置が、得られた出所由来を表す公開鍵に対応する仮想通信路資源群の1つに通信路資源を割り当て、仮想通信路資源を使い通信路を提供することを特徴とする。

【0060】さらにまた、本発明のプログラムID通信範囲制御方法は、仮想通信路用資源群が仮想的に定義したソケットであり、該仮想通信路資源群の一つ一つが該仮想的に定義したソケットの各ポートに対応し、通信路用資源群が通常のソケットであり、各通信路資源群の一つ一つが該通常のソケット各ポートに対応することを特徴とする。

【0061】一方、本発明の公開鍵毎通信路提供方法は、プログラムと、該プログラムを元にプロセスを生成し実行および通信するプログラム実行・通信装置とにより構成される情報システムにおいて、前記プログラム実行・通信装置が、前記プログラムを元に生成および実行されるプロセスとを含み、前記プログラムが、プログラム本体と、該プログラムの出所由来を表す公開鍵と、通信路1つあたりに仮想的に複数の仮想通信路を形成する通信装置と、前記プログラムの出所由来を表す公開鍵毎に1つ以上存在する仮想通信路用資源と、1つ以上の通信路用資源とを含み、前記プログラム実行・通信装置が前記プログラムを元に生成されたプロセスの処理により通信を行う際に、出所由来を表す公開鍵と要求された仮想通信路用資源とを対にして仮想通信路と対応させ、仮想通信路を使い通信路を提供する工程をを含むことを特

徴とする。

【００６２】さらにまた、本発明の公開鍵毎通信路提供方法は、仮想通信路用資源群が仮想的に定義したソケットであり、該仮想通信路資源群の一つ一つが該仮想的に定義したソケットの各ポートに対応し、通信路用資源群が通常のソケットであり、各通信路資源群の一つ一つが該通常のソケット各ポートに対応することを特徴とする。

【００６３】

【発明の実施の形態】以下、本発明の実施の形態について図面を参照して詳細に説明する。

【００６４】（１） 第１の実施の形態

図１を参照すると、本発明の第１の実施の形態に係る秘密鍵なしプログラム認証方法が適用された情報システムは、実行機能および通信機能を有するプログラム実行・通信装置が適用された携帯機器１１と、通信機能を有する通信・処理装置が適用された親機器１２と、携帯機器１１にインストールされて実行されるプログラム１１２とから、その主要部が構成されている。

【００６５】実行機能および通信機能は、Ｊａｖａ（サンマイクロシステムズ社の登録商標）などが想定される。

【００６６】携帯機器１１としては、携帯電話機（ＰＨＳ（Ｐｅｒｓｏｎａｌ　ＨａｎｄｙＰｈｏｎｅ）を含む），携帯情報端末等が想定される。

【００６７】親機器１２としては、ＰＯＳ（Ｐｏｉｎｔ　Ｏｆ　Ｓａｌｅｓ）端末等が想定される。

【００６８】携帯機器１１と親機器１２との間の通信機能は、エリクソン社等が提唱するＢｌｕｅｔｏｏｔｈ，無線ＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ），ＰＩＡＦＳ（ＰＨＳ　Ｉｎｔｅｒｎｅｔ　Ａｃｃｅｓｓ　Ｆｏｒｕｍ　Ｓｔａｎｄａｒｄ）等の近距離無線通信技術で実現されるものとする。

【００６９】携帯機器１１は、信頼できる組み込み機能部１１１と、プログラム１１２を実行するプロセス１１２０と、携帯機器１１に付随する秘密鍵１１３１および公開鍵１１３２とを含んで構成されている。

【００７０】プログラム１１２は、プログラム本体１１２１と、プログラム１１２の出所由来を表す公開鍵１１２２１と、プログラム本体１１２１をハッシュ関数でハッシングしたダイジェストを公開鍵１１２２１と対をなす秘密鍵（図示せず）で暗号化した署名（デジタル署名，電子署名）であるハッシュ値１１２３１とを含んで構成されている。なお、プログラム１１２は、その出所（製造元等）および由来（バージョン等）において、プログラム本体１１２１，公開鍵１１２２１，およびハッシュ値１１２３１が一体として作成されている。

【００７１】親機器１２は、通信してよい相手を示す公開鍵として、携帯機器１１に付随する公開鍵１１３２をもつ。

【００７２】図２を参照すると、携帯機器１１の組み込み機能部１１１および親機器１２の処理は、ハッシュ値確認ステップＳ１０１と、通信要求発生ステップＳ１０２と、携帯機器認証ステップＳ１０３と、プログラム出所由来判定ステップＳ１０４と、プログラム認証ステップＳ１０５と、プログラム不認証ステップＳ１０６とからなる。

【００７３】次に、このように構成された第１の実施の形態に係る秘密鍵なしプログラム認証方法が適用された情報システムの動作について、図１および図２を参照して詳細に説明する。

【００７４】まず、携帯機器１１は、組み込み機能部１１１により、ハッシュ値１１２３１がプログラム本体１１２１および公開鍵１１２２１と対をなす秘密鍵とによって生成されたものであるかどうかを確認する（ステップＳ１０１）。詳しくは、組み込み機能部１１１は、ハッシュ値１１２３１を公開鍵１１２２１で復号してプログラム本体１１２１をハッシングしたダイジェストを得る一方、プログラム本体１１２１を既知のハッシュ関数でハッシングしてダイジェストを得、両ダイジェストが完全に一致するかどうかを検証することで、ハッシュ値１１２３１がプログラム本体１１２１および公開鍵１１２２１と対をなす秘密鍵とによって生成されたものであるかどうかを確認する。すなわち、プログラム本体１１２１および公開鍵１１２２１が改竄されたものでなく、プログラム１１２が真正な出所由来をもつことを確認する。なお、この確認処理は、携帯機器１１にプログラム１１２が導入、たとえばダウンロードされたときに１回行われればよい。

【００７５】次に、携帯機器１１内のプログラム１１２を実行するプロセス１１２０が親機器１２と通信をしようとして通信要求を発生させた場合（ステップＳ１０２）、またはそれ以前に、親機器１２は、携帯機器１１に付随する公開鍵１１３２および秘密鍵１１３１を用いた公開鍵方式により携帯機器１１の認証を行う（ステップＳ１０３）。

【００７６】たとえば、親機器１２は、自らが通信してよい相手を示す公開鍵として保持する携帯機器１１に付随する公開鍵１１３２と、携帯機器１１が保持する携帯機器１１に付随する公開鍵１１３２とが一致するかどうかを判定し、一致した場合に携帯機器１１の認証をおこなう。

【００７７】また、ＲＳＡ（Ｒｉｖｅｓｔ，Ｓｈａｍｉｒ，Ａｄｌｅｍａｎ）の公開鍵によるワン・タイム・パスワード（Ｏｎｅ　Ｔｉｍｅ　Ｐａｓｓｗｏｒｄ）方式を用いた場合、親機器１２は携帯機器１１にランダムな文字列を送り（”Ｃｈａｌｌｅｎｇｅ”）、携帯機器１１の組み込み機能部１１１はその文字列を携帯機器１１に付随する秘密鍵１１３１で暗号化して親機器１２に送り返し（”Ｒｅｓｐｏｎｓｅ”）、親機器１２は暗号化

した文字列を事前に通信してよい相手を示す公開鍵として保持する携帯機器１１に付随する公開鍵１１３２で復号し、復号した文字列と先に送ったランダムな文字列とが一致すれば、携帯機器１１を通信してよい相手（つまり、通信してよい相手を示す公開鍵として保持する携帯機器１１に付随する公開鍵１２３２と対をなす秘密鍵１１３１を所有するもの）であると認証する。

【００７８】携帯機器１１の認証に成功した場合、親機器１２は、携帯機器１１の組み込み機能部１１１から携帯機器１１によるハッシュ値確認結果の公開鍵１１２２１を得、携帯機器１１によるハッシュ値確認結果に基づいてプログラム１１２が真正な出所由来をもつものであるかどうかを判定し（ステップＳ１０４）、そうであれば得られた公開鍵１１２２１でプログラム１１２を認証したとする（ステップＳ１０５）。

【００７９】一方、携帯機器１１の認証に失敗した場合（ステップＳ１０３）、または公開鍵１１２２１がプログラム１１２の真正な出所由来を表す公開鍵でなかった場合（ステップＳ１０４）、親機器１２は、プログラム１１２を認証しない。

【００８０】第１の実施の形態によれば、プログラム１１２が秘密鍵をもたなくても、親機器１２は、親機器１２と通信をしようとしてきた携帯機器１１内のプロセス１１２０の元となるプログラム１１２の認証が可能であることから、盗み見や改竄が可能な環境下にあるプログラム１１２を元にして動作する携帯機器１１と通信を行う場合に、親機器１２がプログラム１１２の成りすましを防止しかつ認証を行うことができる。

【００８１】（２）　第２の実施の形態

図３を参照すると、本発明の第２の実施の形態に係る秘密鍵なしプログラム認証方法が適用された情報システムは、実行機能および通信機能を有するプログラム実行・通信装置が適用された携帯機器２１と、通信機能を有する通信・処理装置が適用された親機器２２と、携帯機器２１にインストールされて実行されるプログラム２１２とから、その主要部が構成されている。

【００８２】実行機能および通信機能は、Ｊａｖａなどが想定される。

【００８３】携帯機器２１としては、携帯電話機（ＰＨＳを含む），携帯情報端末等が想定される。

【００８４】親機器２２としては、ＰＯＳ端末等が想定される。

【００８５】携帯機器２１と親機器２２との間の通信機能は、エリクソン社等が提唱するＢｌｕｅｔｏｏｔｈ，無線ＬＡＮ，ＰＩＡＦＳ等の近距離無線通信技術で実現されるものとする。

【００８６】携帯機器２１は、信頼できる組み込み機能部２１１と、プログラム２１２を実行するプロセス２１２０と、携帯機器２１に付随する秘密鍵２１３１および公開鍵２１３２とを含んで構成されている。

【００８７】プログラム２１２は、プログラム本体２１２１と、プログラム２１２の出所由来を表す公開鍵群２１２２１～２１２２ｎ（ｎは２以上の正整数。以下同様）と、プログラム本体２１２１および公開鍵群２１２２１～２１２２ｎを組み合わせて作成されたデータをハッシュ関数でハッシングしたダイジェストを各公開鍵２１２２１～２１２２ｎと対をなす各秘密鍵（図示せず）でそれぞれ暗号化した署名群であるハッシュ値群２１２３１～２１２３ｎとを含んで構成されている。なお、プログラム２１２は、その出所（製造元等）および由来（バージョン等）において、プログラム本体２１２１，公開鍵群２１２２１～２１２２ｎ，およびハッシュ値群２１２３１～２１２３ｎが一体として作成されている。

【００８８】親機器２２は、通信してよい相手を示す公開鍵として、携帯機器２１に付随する公開鍵２１３２をもつ。

【００８９】図４を参照すると、携帯機器２１の組み込み機能部２１１および親機器２２の処理は、ハッシュ値確認ステップＳ２０１と、通信要求発生ステップＳ２０２と、携帯機器認証ステップＳ２０３と、プログラム由来判定ステップＳ２０４と、プログラム認証ステップＳ２０５と、プログラム不認証ステップＳ２０６とからなる。

【００９０】次に、このように構成された第２の実施の形態に係る秘密鍵なしプログラム認証方法が適用された情報システムの動作について、図３および図４を参照して詳細に説明する。

【００９１】まず、携帯機器２１は、組み込み機能部２１１により、各ハッシュ値２１２３１～２１２３ｎがプログラム本体２１２１および公開鍵群２１２２１～２１２２ｎと各公開鍵２１２２１～２１２２ｎと対をなす各秘密鍵とによって生成されたものであるかどうかを確認し、確認したハッシュ値に対応する公開鍵の集まりを得る（ステップＳ２０１）。詳しくは、組み込み機能部２１１は、各ハッシュ値２１２３１～２１２３ｎを各公開鍵２１２２１～２１２２ｎでそれぞれ復号してプログラム本体２２２１および公開鍵群２１２２１～２１２２ｎを組み合わせて作成されたデータをハッシングしたダイジェスト群を得る一方、プログラム本体２１２１および公開鍵群２１２２１～２１２２ｎを組み合わせて作成されたデータを既知のハッシュ関数でハッシングしてダイジェストを得、該ダイジェストとダイジェスト群の一つ一つとが完全に一致するかどうかをそれぞれ検証することで、各ハッシュ値２１２３１～２１２３ｎがプログラム本体２１２１および公開鍵群２１２２１～２１２２ｎと各公開鍵２１２２１～２１２２ｎと対をなす各秘密鍵とによって生成されたものであるかどうかをそれぞれ確認し、確認したハッシュ値に対応する公開鍵の集まりを得る。すなわち、プログラム本体２１２１および公開鍵群２１２２１～２１２２ｎが、改竄されたものでなく、

プログラム２１２が真正な出所由来をもつことを確認する。なお、この確認処理は、携帯機器２１にプログラム２１２が導入、たとえばダウンロードされたときに１回行われればよい。

【００９２】次に、携帯機器２１内のプログラム２１２を実行するプロセス２１２０が親機器２２と通信をしようとして通信要求が発生した場合(ステップＳ２０２)、またはそれ以前に、親機器２２は、携帯機器２１に付随する秘密鍵２１３１および公開鍵２１３２を用いた公開鍵方式により携帯機器２１の認証を行う（ステップＳ２０３）。

【００９３】たとえば、親機器２２は、自らが通信してよい相手を示す公開鍵として保持する携帯機器２１に付随する公開鍵２１３２と、携帯機器２１が保持する携帯機器２１に付随する公開鍵２１３２とが一致するかどうかを判定し、一致した場合に携帯機器２１の認証を行う。

【００９４】また、ＲＳＡの公開鍵によるワン・タイム・パスワード方式を用いた場合、親機器２２は携帯機器２１にランダムな文字列を送り（"Ｃｈａｌｌｅｎｇｅ"）、携帯機器２１の組み込み機能部２１１はその文字列を携帯機器２１に付随する秘密鍵２１３１で暗号化して親機器２２に送り返し（"Ｒｅｓｐｏｎｓｅ"）、親機器２２は暗号化した文字列を事前に通信してよい相手を示す公開鍵として保持する携帯機器２１に付随する公開鍵２１３２で復号し、復号した文字列と先に送ったランダムな文字列とが一致すれば、携帯機器２１を通信してよい相手（つまり、通信してよい相手を示す公開鍵として保持する携帯機器２１に付随する公開鍵２１３２と対をなす秘密鍵２１３１を所有するもの）であると認証する。

【００９５】携帯機器２１の認証に成功した場合、親機器２２は、携帯機器２１の組み込み機能部２１１から携帯機器２１によるハッシュ値確認結果の公開鍵の集まりを得、携帯機器２１によるハッシュ値確認結果の公開鍵の集まりに１つ以上の公開鍵が含まれていればプログラム２１２が真正な出所由来をもつものであると判定し（ステップＳ２０４）、公開鍵の集まりの一部または全部でプログラム２１２を認証したとする（ステップＳ２０５）。

【００９６】一方、携帯機器２１の認証に失敗した場合（ステップＳ２０３）、またはプログラム２１２の真正な出所由来を表す公開鍵が得られなかった場合（ステップＳ２０４）、親機器２２は、プログラム２１２を認証しない（ステップＳ２０６）。

【００９７】なお、上記第２の実施の形態では、ステップＳ２０４で携帯機器２１によるハッシュ値確認結果の公開鍵の集まりに１つ以上の公開鍵が含まれていればプログラム２１２が真正な出所由来をもつものであると判定したが、携帯機器２１によるハッシュ値確認結果の公開鍵の集まりに公開鍵群２１２２１～２１２２ｎのすべてが含まれていたときにのみプログラム２１２が真正な出所由来をもつものであると判定するようにすることもできる。

【００９８】第２の実施の形態によれば、プログラム２１２が公開鍵群２１２２１～２１２２ｎをもつことを許す場合は、プログラム本体２１２１とともに保持する公開鍵群２１２２１～２１２２ｎに対し署名群であるハッシュ値群２１２３１～２１２３ｎを付与することから、プログラムの成りすましを防止することができる。

【００９９】（２） 第３の実施の形態

図５を参照すると、本発明の第３の実施の形態に係るプログラムＩＤ通信処理制御方法が適用された情報システムは、実行機能および通信機能を有するプログラム実行・通信装置が適用された携帯機器３１と、通信機能を有する通信・処理装置が適用された親機器３２と、携帯機器３１にインストールされて実行されるプログラム３１２とから、その主要部が構成されている。

【０１００】実行機能および通信機能は、Ｊａｖａなどが想定される。

【０１０１】携帯機器３１としては、携帯電話機（ＰＨＳを含む），携帯情報端末等が想定される。

【０１０２】親機器３２としては、ＰＯＳ端末等が想定される。

【０１０３】携帯機器３１と親機器３２との間の通信機能は、エリクソン社等が提唱するＢｌｕｅｔｏｏｔｈ，無線ＬＡＮ，ＰＩＡＦＳ等の近距離無線通信技術で実現されるものとする。

【０１０４】携帯機器３１は、信頼できる組み込み機能部３１１と、プログラム３１２を実行するプロセス３１２０とを含んで構成されている。

【０１０５】プログラム３１２は、プログラム本体３１２１と、プログラム３１２の出所由来を表す公開鍵３１２２１および秘密鍵３１２４１とを含んで構成されている。なお、プログラム３１２は、その出所（製造元等）および由来（バージョン等）において、プログラム本体３１２１，公開鍵３１２２１，および秘密鍵３１２４１が一体として作成されている。

【０１０６】図６を参照すると、携帯機器３１の組み込み機能部３１１および親機器３２の処理は、通信要求発生ステップＳ３０１と、公開鍵獲得ステップＳ３０２と、プログラム認証ステップＳ３０３と、通信・処理ステップＳ３０４と、通信・処理なしステップＳ３０５とからなる。

【０１０７】次に、このように構成された第３の実施の形態に係るプログラムＩＤ通信処理制御方法が適用された情報システムの動作について、図５および図６を参照して詳細に説明する。

【０１０８】携帯機器３１内のプログラム３１２を実行するプロセス３１２０が親機器３２と通信するための通

信要求を発生させた場合（ステップＳ３０１）、親機器３２は、携帯機器３１の組み込み機能部３１１を介して、プロセス３１２０の元となるプログラム３１２の出所由来を表す公開鍵３１２２１を得る（ステップＳ３０２）。

【０１０９】次に、親機器３２は、携帯機器３１の組み込み機能部３１１に対し、公開鍵３１２２１および秘密鍵３１２４１を用いた公開鍵方式によりプロセス３１２０の元となるプログラム３１２が真正な出所由来をもつものであるかどうかを認証する（ステップＳ３０３）。

【０１１０】たとえば、ＲＳＡの公開鍵によるワン・タイム・パスワード方式を用いた場合、親機器３２は携帯機器３１の組み込み部３１１にランダムな文字列を送り（"Ｃｈａｌｌｅｎｇｅ"）、携帯機器３１の組み込み機能部３１１はその文字列をプロセス３１２０の元となるプログラム３１２の出所由来を表す公開鍵３１２２１と対をなす秘密鍵３１２４１で暗号化して親機器３２に送り返し（"Ｒｅｓｐｏｎｓｅ"）、親機器３２は暗号化した文字列を先に受け取った公開鍵３１２２１で復号し、復号した文字列と先に送ったランダムな文字列とが一致すれば、プロセス３１２０の元となるプログラム３１２は真正な出所由来をもつものである（つまり、プログラム３１２が該プログラム３１２の出所由来を表す公開鍵３１２２１と対をなす秘密鍵３１２４１を所有する）と認証する。

【０１１１】プログラム３１２の認証に成功した場合（ステップＳ３０３）、親機器３２は、以降の通信によって発生する処理を、公開鍵３１２２１に対応するユーザ権限でアクセス制御して実行する（ステップＳ３０４）。

【０１１２】一方、プログラム３１２の認証に失敗した場合（ステップＳ３０３）、または公開鍵３１２２１に対応するユーザ権限が存在しない場合、親機器３２は、通信によって発生する処理をしないか、特定の制限されたユーザ権限で処理を実行する（ステップＳ３０５）。

【０１１３】第３の実施の形態によれば、プログラム３１２の出所由来を表す公開鍵３１２２１、つまりプログラム３１２の製造元やバージョンに類する情報を元にしたアクセス制御により通信を行うことから、悪意のプログラムに対しセキュリティを保つことができる。

【０１１４】また、プログラム３１２の出所由来を表す公開鍵３１２２１、つまりプログラム３１２の製造元やバージョンに類する情報を元にしたアクセス制御により通信を行うため、ユーザ管理のような集中管理が困難な分散環境下での通信による処理について、悪意のプログラムに対しセキュリティを保つことができる。

【０１１５】（４）　第４の実施の形態

図７を参照すると、本発明の第４の実施の形態に係るプログラムＩＤ通信処理制御方法が適用された情報システムは、実行機能および通信機能を有するプログラム実行・通信装置が適用された携帯機器４１と、通信機能を有する通信・処理装置が適用された親機器４２と、携帯機器４１にインストールされ実行されるプログラム４１２とから、その主要部が構成されている。

【０１１６】実行機能および通信機能は、Ｊａｖａなどが想定される。

【０１１７】携帯機器４１としては、携帯電話機（ＰＨＳを含む），携帯情報端末等が想定される。

【０１１８】親機器４２としては、ＰＯＳ端末等が想定される。

【０１１９】携帯機器４１と親機器４２との間の通信機能は、エリクソン社等が提唱するＢｌｕｅｔｏｏｔｈ，無線ＬＡＮ，ＰＩＡＦＳ等の近距離無線通信技術で実現されるものとする。

【０１２０】携帯機器４１は、信頼できる組み込み機能部４１１と、プログラム４１２を実行するプロセス４１２０と、携帯機器４１に付随する秘密鍵４１３１および公開鍵４１３２とを含んで構成されている。

【０１２１】プログラム４１２は、プログラム本体４１２１と、プログラム４１２の出所由来を表す公開鍵４１２２１と、プログラム本体４１２１をハッシュ関数でハッシングしたダイジェストを公開鍵４１２２１と対をなす秘密鍵（図示せず）で暗号化した署名であるハッシュ値４１２３１とを含んで構成されている。なお、プログラム４１２は、その出所（製造元等）および由来（バージョン等）において、プログラム本体４１２１，公開鍵４１２２１，およびハッシュ値４１２３１が一体として作成されている。

【０１２２】親機器４２は、通信してよい相手を示す公開鍵として、携帯機器４１に付随する公開鍵４１３２をもつ。

【０１２３】図８を参照すると、携帯機器４１の組み込み機能部４１１および親機器４２の処理は、ハッシュ値確認ステップＳ４０１と、通信要求発生ステップＳ４０２と、携帯機器認証ステップＳ４０３と、プログラム出所由来判定ステップＳ４０４と、通信・処理ステップＳ４０５と、通信・処理なしステップＳ４０６とからなる。

【０１２４】次に、このように構成された第４の実施の形態に係るプログラムＩＤ通信処理制御方法が適用された情報システムの動作について、図７および図８を参照して詳細に説明する。

【０１２５】まず、携帯機器４１は、組み込み機能部４１１により、ハッシュ値４１２３１がプログラム本体４１２１および公開鍵４１２２１と対をなす秘密鍵とによって生成されたものであるかどうかを確認する（ステップＳ４０１）。詳しくは、組み込み機能部４１１は、ハッシュ値４１２３１を公開鍵４１２２１で復号してプログラム本体４１２１をハッシングしたダイジェストを得る一方、プログラム本体４１２１を既知のハッシュ関数

でハッシングしてダイジェストを得、両ダイジェストが完全に一致するかどうかを検証することで、ハッシュ値４１２３１がプログラム本体４１２１および公開鍵４１２２１と対をなす秘密鍵とによって生成されたものであるかどうかを確認する。すなわち、プログラム本体４１２１および公開鍵４１２２１が改竄されたものでなく、プログラム４１２が真正な出所由来をもつことを確認する。なお、この確認処理は、携帯機器４１にプログラム４１２が導入、たとえばダウンロードされたときに１回行われればよい。

【０１２６】次に、携帯機器４１内のプログラム４１２を実行するプロセス４１２０が親機器４２と通信をしようとして通信要求を発生させた場合（ステップＳ４０２）、またはそれ以前に、親機器４２は、携帯機器４１に付随する公開鍵４１３２および秘密鍵４１３１を用いた公開鍵方式により携帯機器４１の認証を行う（ステップＳ４０３）。

【０１２７】たとえば、親機器４２は、自らが通信してよい相手を示す公開鍵として保持する携帯機器４１に付随する公開鍵４１３２と、携帯機器４１が保持する携帯機器４１に付随する公開鍵４１３２とが一致するかどうかを判定し、一致した場合に携帯機器４１を認証する。

【０１２８】また、ＲＳＡの公開鍵によるワン・タイム・パスワード方式を用いた場合、親機器４２は携帯機器４１にランダムな文字列を送り（"Ｃｈａｌｌｅｎｇｅ"）、携帯機器４１の組み込み機能部４１１はその文字列を携帯機器４１に付随する秘密鍵４１３１で暗号化して親機器４２に送り返し（"Ｒｅｓｐｏｎｓｅ"）、親機器４２は暗号化した文字列を事前に通信してよい相手を示す公開鍵として保持する携帯機器４１に付随する公開鍵４１３２で復号し、復号した文字列と先に送ったランダムな文字列とが一致すれば、携帯機器４１を通信してよい相手（つまり、通信してよい相手を示す公開鍵として保持する携帯機器４１に付随する公開鍵４１３２と対をなす秘密鍵４１３１を所有するもの）であると認証する。

【０１２９】携帯機器４１の認証に成功した場合、親機器４２は、携帯機器４１の組み込み機能部４１１から公開鍵４１２２１を得、携帯機器４１によるハッシュ値確認結果に基づいてプログラム４１２が真正な出所由来をもつものであるかどうかを判定し（ステップＳ４０４）、そうであれば以降の通信によって発生する処理を公開鍵４１２２１に対応するユーザ権限でアクセス制御して実行する（ステップＳ４０５）。

【０１３０】一方、携帯機器４１の認証に失敗した場合（ステップＳ４０３）、プログラム４１２が真正な出所由来をもつものでなかった場合（ステップＳ４０４）、または公開鍵４１２２１に対応するユーザ権限が存在しない場合、親機器４２は、通信によって発生する処理を実行しないか、特定の決められたユーザ権限でアクセス制御して実行する（ステップＳ４０６）。

【０１３１】第４の実施の形態によれば、プログラム４１２が秘密鍵をもたなくても、親機器４２は、親機器４２と通信をしようとしてきた携帯機器４１内のプロセス４１２０の元となるプログラム４１２の認証が可能であることから、盗み見や改竄が可能な環境下にあるプログラム４１２を元にして動作する携帯機器４１と通信を行う場合に、親機器４２がプログラム４１２の成りすましを防止しかつ認証を行うことができる。

【０１３２】（５）　第５の実施の形態

図９を参照すると、本発明の第５の実施の形態に係るプログラムＩＤ通信処理制御方法が適用された情報システムは、実行機能および通信機能を有するプログラム実行・通信装置が適用された携帯機器５１と、通信機能を有する通信・処理装置が適用された親機器５２と、携帯機器５１にインストールされ実行されるプログラム５１２とから、その主要部が構成されている。

【０１３３】実行機能および通信機能は、Ｊａｖａなどが想定される。

【０１３４】携帯機器５１としては、携帯電話機（ＰＨＳを含む），携帯情報端末等が想定される。

【０１３５】親機器５２としては、ＰＯＳ端末等が想定される。

【０１３６】携帯機器５１と親機器５２との間の通信機能は、エリクソン社等が提唱するＢｌｕｅｔｏｏｔｈ，無線ＬＡＮ，ＰＩＡＦＳ等の近距離無線通信技術で実現されるものとする。

【０１３７】携帯機器５１は、信頼できる組み込み機能部５１１と、プログラム５１２を実行するプロセス５１２０と、携帯機器５１に付随する秘密鍵５１３１および公開鍵５１３２とを含んで構成されている。

【０１３８】プログラム５１２は、プログラム本体５１２１と、プログラム５１２の出所由来を表す公開鍵群５１２２１～５１２２ｎと、プログラム本体５１２１および公開鍵群５１２２１～５１２２ｎを組み合わせて作成されたデータをハッシュ関数でハッシングしたダイジェストを各公開鍵５１２２１～５１２２ｎと対をなす各秘密鍵（図示せず）でそれぞれ暗号化した署名群であるハッシュ値群５１２３１～５１２３ｎとを含んで構成されている。なお、プログラム５１２は、その出所（製造元等）および由来（バージョン等）において、プログラム本体５１２１，公開鍵群５１２２１～５１２２ｎ，およびハッシュ値群５１２３１～５１２３ｎが一体として作成されている。

【０１３９】親機器５２は、通信してよい相手を示す公開鍵として、携帯機器５１に付随する公開鍵５１３２をもつ。

【０１４０】図１０を参照すると、携帯機器５１の組み込み機能部５１１および親機器５２の処理は、ハッシュ値確認ステップＳ５０１と、通信要求発生ステップＳ５

０２と、携帯機器認証ステップＳ５０３と、プログラム出所由来判定ステップＳ５０４と、通信・処理ステップＳ５０５と、通信・処理なしステップＳ５０６とからなる。

【０１４１】次に、このように構成された第５の実施の形態に係るプログラムＩＤ通信処理制御方法が適用された情報システムの動作について、図９および図１０を参照して詳細に説明する。

【０１４２】まず、携帯機器５１は、組み込み機能部５１１により、各ハッシュ値５１２３１～５１２３ｎがプログラム本体５１２１および公開鍵群５１２２１～５１２２ｎと各公開鍵５１２２１～５１２２ｎと対をなす各秘密鍵とによって生成されたものであるかどうかを確認し、確認したハッシュ値に対応する公開鍵の集まりを得る（ステップＳ５０１）。詳しくは、組み込み機能部５１１は、各ハッシュ値５１２３１～５１２３ｎを各公開鍵５１２２１～５１２２ｎでそれぞれ復号してプログラム本体５１２１および公開鍵群５１２２１～５１２２ｎを組み合わせて作成されたデータをハッシングしたダイジェスト群を得る一方、プログラム本体５１２１および公開鍵群５１２２１～５１２２ｎを組み合わせて作成されたデータを既知のハッシュ関数でハッシングしてダイジェストを得、該ダイジェストとダイジェスト群の一つ一つとが完全に一致するかどうかをそれぞれ検証することで、各ハッシュ値５１２３１～５１２３ｎがプログラム本体５１２１および公開鍵群５１２２１～５１２２ｎと各公開鍵５１２２１～５１２２ｎと対をなす各秘密鍵とによって生成されたものであるかどうかをそれぞれ確認し、確認したハッシュ値に対応する公開鍵の集まりを得る。すなわち、プログラム本体５１２１および公開鍵群５１２２１～５１２２ｎが、改竄されたものでなく、プログラム５１２が真正な出所由来をもつことを確認する。なお、この確認処理は、携帯機器５１にプログラム５１２が導入、たとえばダウンロードされたときに１回行われればよい。

【０１４３】次に、携帯機器５１内のプログラム５１２を実行するプロセス５１２０が親機器５２と通信をしようとして通信要求が発生した場合(ステップＳ５０２)、またはそれ以前に、親機器５２は、携帯機器５１に付随する公開鍵５１３２および秘密鍵５１３１を用いた公開鍵方式により携帯機器５１の認証を行う（ステップＳ５０３）。

【０１４４】たとえば、親機器５２は、自らが通信してよい相手を示す公開鍵として保持する携帯機器５１に付随する公開鍵５１３２と、携帯機器５１が保持する携帯機器５１に付随する公開鍵５１３２とが一致するかどうかを判定し、一致した場合に携帯機器５１の認証を行う。

【０１４５】また、ＲＳＡの公開鍵によるワン・タイム・パスワード方式を用いた場合、親機器５２は携帯機器５１にランダムな文字列を送り（”Ｃｈａｌｌｅｎｇｅ”）、携帯機器５１の組み込み機能部５１１はその文字列を携帯機器５１に付随する秘密鍵５１３１で暗号化して親機器５２に送り返し（”Ｒｅｓｐｏｎｓｅ”）、親機器５２は暗号化した文字列を事前に通信してよい相手を示す公開鍵として保持する携帯機器５１に付随する公開鍵５１３２で復号し、復号した文字列と先に送ったランダムな文字列とが一致すれば、携帯機器５１を通信してよい相手（つまり、通信してよい相手を示す公開鍵として保持する携帯機器５１に付随する公開鍵５１３２と対をなす秘密鍵５１３１を所有するもの）であると認証する。

【０１４６】携帯機器５１の認証に成功した場合、親機器５２は、携帯機器５１の組み込み機能部５１１からハッシュ値確認結果の公開鍵の集まりを得、携帯機器５１によるハッシュ値確認結果の公開鍵の集まりに１つ以上の公開鍵が含まれていればプログラム５１２が真正な出所由来をもつものであると判定し（ステップＳ５０４）、以降の通信によって発生する処理をハッシュ値確認結果の公開鍵の集まりの各公開鍵に対応するユーザ権限の組み合わせでアクセス制御して実行する（ステップＳ５０５）。

【０１４７】一方、携帯機器５１の認証に失敗した場合（ステップＳ５０３）、プログラム５１２が真正な出所由来をもつものでない場合（ステップＳ５０４）、または携帯機器５１によるハッシュ値確認結果の公開鍵の集まり中の公開鍵に対応するユーザ権限が１つも存在しない場合、親機器５２は、通信によって発生する処理を実行しないか、特定の制限されたユーザ権限でアクセス制御して実行する（ステップＳ５０６）。

【０１４８】なお、上記第５の実施の形態では、ステップＳ５０４で携帯機器５１によるハッシュ値確認結果の公開鍵の集まりに１つ以上の公開鍵が含まれていればプログラム５１２が真正な出所由来をもつものであると判定したが、携帯機器５１によるハッシュ値確認結果の公開鍵の集まりに公開鍵群５１２２１～５１２２ｎのすべてが含まれていたときにのみプログラム５１２が真正な出所由来をもつものであると判定するようにすることもできる。

【０１４９】第５の実施の形態によれば、プログラム５１２が該プログラム５１２の出所由来を表す公開鍵群５１２２１～５１２２ｎをもつことを許す場合はプログラム本体５１２１とともに保持する公開鍵群５１２２１～５１２２ｎに対して署名群であるハッシュ値群５１２３１～５１２３ｎを付すことから、プログラム５１２の成りすましを防止することができ、通信によって発生する処理をハッシュ値確認結果の公開鍵の集まりの各公開鍵に対応するユーザ権限の組み合わせでアクセス制御して実行することができる。

【０１５０】（６）　第６の実施の形態

図１１を参照すると、本発明の第６の実施の形態に係るプログラムＩＤ通信範囲制御方法が適用された情報システムは、プログラムの実行機能および通信機能を有する携帯機器６１と、同じくプログラムの実行機能および通信機能を有する親機器６２と、携帯機器６１にインストールされ実行されるプログラム６１２と、親機器６２にインストールされ実行されるプログラム６２２とから、その主要部が構成されている。

【０１５１】実行機能および通信機能は、Ｊａｖａなどが想定される。

【０１５２】携帯機器６１としては、携帯電話機（ＰＨＳを含む），携帯情報端末等が想定される。

【０１５３】親機器６２としては、ＰＯＳ端末等が想定される。

【０１５４】携帯機器６１と親機器６２との間の通信機能に使用される通信方式は、エリクソン社等が提唱するＢｌｕｅｔｏｏｔｈ，無線ＬＡＮ，ＰＩＡＦＳ等の近距離無線通信技術で実現されるものとする。

【０１５５】携帯機器６１は、信頼できる組み込み機能部６１１と、プログラム６１２を実行するプロセス６１２０とを含んで構成されている。

【０１５６】プログラム６１２は、プログラム本体６１２１と、プログラム６１２の出所由来を表す公開鍵６１２２および秘密鍵６１２４とを含んで構成されている。なお、プログラム６１２は、その出所（製造元等）および由来（バージョン等）において、プログラム本体６１２１，公開鍵６１２２および秘密鍵６１２４が一体として作成されている。

【０１５７】親機器６２は、信頼できる組み込み機能部６２１と、プログラム６２２を実行するプロセス６２２０とを含んで構成されている。

【０１５８】プログラム６２２は、プログラム本体６２２１と、プログラム６２２の出所由来を表す公開鍵６２２２および秘密鍵６２２４とを含んで構成されている。なお、プログラム６２２は、その出所（製造元等）および由来（バージョン等）において、プログラム本体６２２１，公開鍵６２２２および秘密鍵６２２４が一体として作成されている。

【０１５９】図１２を参照すると、携帯機器６１の組み込み機能部６１１および親機器６２の組み込み機能部６２１の処理は、通信要求発生ステップＳ６０１と、公開鍵獲得ステップＳ６０２と、相互認証ステップＳ６０３と、公開鍵比較ステップＳ６０４と、相互認証・公開鍵一致判定ステップＳ６０５と、通信許可ステップＳ６０６と、通信不許可ステップＳ６０７とからなる。

【０１６０】次に、このように構成された第６の実施の形態に係るプログラムＩＤ通信範囲制御方法が適用された情報システムの動作について、図１１および図１２を参照して詳細に説明する。

【０１６１】携帯機器６１内のプログラム６１２を実行するプロセス６１２０と親機器６２内のプログラム６２２を実行するプロセス６２２０との間で通信要求が発生した場合（ステップＳ６０１）、まず、携帯機器６１の組み込み機能部６１１は、親機器６２の組み込み機能部６２１にプロセス６１２０の元となるプログラム６１２の出所由来を表す公開鍵６１２２を送り、親機器６２の組み込み機能部６２１は、携帯機器６１の組み込み機能部６１１にプロセス６２２０の元となるプログラム６２２の出所由来を表す公開鍵６２２２を送り(ステップＳ６０２)、次に、双方で、公開鍵６１２２と公開鍵６２２２とが一致するかどうかを調べる(ステップＳ６０３)。

【０１６２】次に、携帯機器６１の組み込み機能部６１１と親機器６２の組み込み機能部６２１との間で、プログラム６１２およびプログラム６２２の相互認証を行う（ステップＳ６０４）。

【０１６３】たとえば、ＲＳＡの公開鍵によるワン・タイム・パスワード方式を用いた場合、携帯機器６１の組み込み機能部６１１は親機器６２の組み込み機能部６２１にランダムな文字列を送り（”Ｃｈａｌｌｅｎｇｅ”）、親機器６２の組み込み機能部６２１はその文字列をプログラム６２２の秘密鍵６２２４で暗号化して携帯機器６１の組み込み機能部６１１に送り返し（”Ｒｅｓｐｏｎｓｅ”）、携帯機器６１の組み込み機能部６１１は、暗号化した文字列を公開鍵６２２２で復号し、復号した文字列と先に送ったランダムな文字列とが一致すれば、プロセス６２２０の元となるプログラム６２２が公開鍵６２２２をもつ（つまり、プロセス６２２０の元となるプログラム６２２が公開鍵６２２２と対をなす秘密鍵６２２４をもつ）と認証する。

【０１６４】一方、親機器６２の組み込み機能部６２１は携帯機器６１の組み込み機能部６１１にランダムな文字列を送り（”Ｃｈａｌｌｅｎｇｅ”）、携帯機器６１の組み込み機能部６１１はその文字列を携帯機器６１に付随する秘密鍵６１２４で暗号化して親機器６２の組み込み機能部６２１に送り返し（”Ｒｅｓｐｏｎｓｅ”）、親機器６２の組み込み機能部６２１は、暗号化した文字列を公開鍵６１２２で復号し、復号した文字列と先に送ったランダムな文字列とが一致すれば、プロセス６１２０の元となるプログラム６１２が公開鍵６１２２をもつ（つまり、プロセス６１２０の元となるプログラム６１２が公開鍵６１２２と対をなす秘密鍵６１２４をもつ）と認証する。

【０１６５】プログラム６１１およびプログラム６１２の相互認証が成功し、かつ公開鍵６１２２と公開鍵６２２２とが一致した場合（ステップＳ６０５）、携帯機器６１の組み込み機能部６１１および親機器６２の組み込み機能部６２１は、プロセス６１２１０とプロセス６２２１０との間で通信を許可する（ステップＳ６０６）。

【０１６６】逆に、プログラム６１１およびプログラム

６１２の相互認証に失敗した場合、あるいはプログラム６１２の出所由来を表す公開鍵６１２２とプログラム６２２の出所由来を表す公開鍵６２２２とが一致しなかった場合、携帯機器６１の組み込み機能部６１１および親機器６２の組み込み機能部６２１は、プロセス６１２０とプロセス６２２０との間で通信を不許可とする（ステップＳ６０７）。

【０１６７】第６の実施の形態によれば、携帯機器６１内のプログラム６１２および親機器６２内のプログラム６２２が、一致する公開鍵６１２２および６２２２を付随するプログラム６１２および６２２としか通信できず、任意の他のプログラムと通信できないため、携帯機器６１内のプログラム６１２および親機器６２内のプログラム６２２のもつ情報の、流通する範囲を出所由来を同じくするプログラムの範囲内に限ることができる。

【０１６８】また、携帯機器６１内のプログラム６１２および親機器６２内のプログラム６２２が、一致する公開鍵６１２２および６２２２を付随するプログラム６１２および６２２としか通信できず、任意の他のプログラムと通信できないため、携帯機器６１内のプログラム６１２および親機器６２内のプログラム６２２のもつ情報が、たとえプログラム６１２および６２２が暴走しても、出所由来を同じくするプログラムの範囲外に漏洩しない。

【０１６９】さらに、分散環境における通信範囲の制御についてのセキュリティ面での設計が容易になり、かつ自由度が変わらないことである。その理由は、分散環境におけるもっとも重要な問題の１つである通信時の情報漏洩について、製造元またはそれに類するものを同じくするプログラムの間でしか情報を流通させないために、設計時に情報の流通範囲を設計しなくても、悪意のある他者への漏洩や、プログラムのバグ，暴走による漏洩が起こらず、また、逆に１つのサービスにおいては、そのプロジェクトにかかわるもの全体である１つの製造元またはそれに類するものとみなすことで、情報の流通を行え、またその流通範囲で十分であるからである。

【０１７０】（７）　第７の実施の形態

図１３を参照すると、本発明の第７の実施の形態に係るプログラムＩＤ通信範囲制御方法が適用された情報システムは、プログラムの実行機能および通信機能を有する携帯機器７１と、同じくプログラムの実行機能および通信機能を有する親機器７２と、携帯機器７１にインストールされ実行されるプログラム７１２と、親機器７２にインストールされ実行されるプログラム７２２とから、その主要部が構成されている。

【０１７１】実行機能および通信機能は、Ｊａｖａなどが想定される。

【０１７２】携帯機器７１としては、携帯電話機（ＰＨＳを含む），携帯情報端末等が想定される。

【０１７３】親機器７２としては、ＰＯＳ端末等が想定される。

【０１７４】携帯機器７１と親機器７２との間の通信機能に使用される通信方式は、エリクソン社等が提唱するＢｌｕｅｔｏｏｔｈ，無線ＬＡＮ，ＰＩＡＦＳ等の近距離無線通信技術で実現されるものとする。

【０１７５】携帯機器７１は、信頼できる組み込み機能部７１１と、プログラム７１２を実行するプロセス７１２０と、携帯機器７１に付随する秘密鍵７１３１および公開鍵７１３２と、親機器７２に付随する公開鍵７２３２とを含んで構成されている。

【０１７６】プログラム７１２は、プログラム本体７１２１と、プログラム７１２の出所由来を表す公開鍵７１２２と、プログラム本体７１２１をハッシュ関数でハッシングしたダイジェストを公開鍵７１２２と対をなす秘密鍵（図示せず）で暗号化した署名であるハッシュ値７１２３とを含んで構成されている。なお、プログラム７１２は、その出所（製造元等）および由来（バージョン等）においてプログラム本体７１２１，公開鍵７１２２，およびハッシュ値７１２３が一体として作成されている。

【０１７７】親機器７２は、信頼できる組み込み機能部７２１と、プログラム７２２を実行するプロセス７２２０と、親機器７２に付随する秘密鍵７２３１および公開鍵７２３２と、携帯機器７１に付随する公開鍵７１３２とを含んで構成されている。

【０１７８】プログラム７２２は、プログラム本体７２２１と、プログラム７２２の出所由来を表す公開鍵７２２２と、プログラム本体７２２１をハッシュ関数でハッシングしたダイジェストを公開鍵７２２２と対をなす秘密鍵（図示せず）で暗号化した署名であるハッシュ値７２２３とを含んで構成されている。なお、プログラム７２２は、その出所（製造元等）および由来（バージョン等）において、プログラム本体７２２１，公開鍵７２２２，およびハッシュ値７２２３が一体として作成されている。

【０１７９】図１４を参照すると、携帯機器７１の組み込み機能部７１１および親機器７２の組み込み機能部７２１の処理は、ハッシュ値確認ステップＳ７０１およびＳ７０２と、通信要求発生ステップＳ７０３と、相互認証ステップＳ７０４と、公開鍵一致判定ステップＳ７０５と、通信許可ステップＳ７０６と、通信不許可ステップＳ７０７とからなる。

【０１８０】次に、このように構成された第７の実施の形態に係るプログラムＩＤ通信範囲制御方法が適用された情報システムの動作について、図１３および図１４を参照して詳細に説明する。

【０１８１】まず、携帯機器７１は、組み込み機能部７１１により、ハッシュ値７１２３がプログラム本体７１２１および公開鍵群７１２２と公開鍵７１２２と対をなす秘密鍵とによって生成されたものであるかどうかを確

認する（ステップＳ７０１）。詳しくは、組み込み機能部７１１は、ハッシュ値７１２３を公開鍵７１２２で復号してプログラム本体７２２１をハッシングしたダイジェストを得る一方、プログラム本体７１２１を既知のハッシュ関数でハッシングしてダイジェストを得、両ダイジェストが完全に一致するかどうかを検証することで、ハッシュ値７１２３がプログラム本体７１２１および公開鍵群７１２２と公開鍵７１２２と対をなす秘密鍵とによって生成されたものであるかどうかを確認する。すなわち、プログラム本体７１２１および公開鍵７１２２が改竄されたものでなく、プログラム７１２が真正な出所由来をもつことを確認する。なお、この確認処理は、携帯機器７１にプログラム７１２が導入、たとえばダウンロードされたときなどに１回行われればよい。

【０１８２】また、親機器７２も、組み込み機能部７２１により、ハッシュ値７２２３がプログラム本体７２２１および公開鍵群７２２２と公開鍵７２２２と対をなす秘密鍵とによって生成されたものであるかどうかを確認する（ステップＳ７０２）。詳しくは、組み込み機能部７２１は、ハッシュ値７２２３を公開鍵７２２２で復号してプログラム本体７２２１をハッシングしたダイジェストを得る一方、プログラム本体７２２１を既知のハッシュ関数でハッシングしてダイジェストを得、両ダイジェストが完全に一致するかどうかを検証することで、ハッシュ値７２２３がプログラム本体７２２１および公開鍵群７２２２と公開鍵７２２２と対をなす秘密鍵とによって生成されたものであることを確認する。すなわち、プログラム本体７２２１および公開鍵７２２２が改竄されたものでなく、プログラム７２２が真正な出所由来をもつことを確認する。なお、この確認処理は、親機器７２にプログラム７２２が導入、たとえばインストールされたときなどに１回行われればよい。

【０１８３】次に、携帯機器７１内のプログラム７１２を実行するプロセス７１２０と親機器７２内のプログラム７２２を実行するプロセス７２２０とが通信をしようとして通信要求が発生した場合（ステップＳ７０３）、またはそれ以前に、まず、携帯機器７１の組み込み機能部７１１と親機器７２の組み込み機能部７２１との間で、携帯機器７１が付随する秘密鍵７１３１および公開鍵７１３２と、親機器７２に付随する秘密鍵７２３１および公開鍵７２３２とを用いた公開鍵方式により携帯機器７１および親機器７２の相互認証を行う（ステップＳ７０４）。

【０１８４】たとえば、親機器７２は、自らが通信してよい相手を示す公開鍵として保持する携帯機器７１に付随する公開鍵７１３２と、携帯機器７１が保持する携帯機器７１に付随する公開鍵７１１３２とが一致するかどうかを判定し、一致した場合に携帯機器７１の認証を行う。一方、携帯機器７１は、自らが通信してよい相手を示す公開鍵として保持する親機器７２に付随する公開鍵７２３２と、親機器７２が保持する親機器７２に付随する公開鍵７２１３２とが一致するかどうかを判定し、一致した場合に親機器７２の認証を行う。

【０１８５】また、ＲＳＡの公開鍵によるワン・タイム・パスワード方式を用いた場合、携帯機器７１の組み込み機能部７１１は親機器７２にランダムな文字列を送り（”Ｃｈａｌｌｅｎｇｅ”）、親機器７２の組み込み機能部７２１はその文字列を親機器７２に付随する秘密鍵７２３１で暗号化して携帯機器７１に送り返し（”Ｒｅｓｐｏｎｓｅ”）、携帯機器７１の組み込み機能部７１１は、暗号化した文字列を親機器７２に付随する公開鍵７２３２で復号し、復号した文字列と先に送ったランダムな文字列とが一致すれば、親機器７２を通信してよい相手（つまり、親機器７２に付随する公開鍵７２３２と対をなす秘密鍵７２３１を所有するもの）であると認証する。一方、親機器７２の組み込み機能部７２１は携帯機器７１にランダムな文字列を送り（”Ｃｈａｌｌｅｎｇｅ”）、携帯機器７１の組み込み機能部７１１はその文字列を携帯機器７１に付随する秘密鍵７１３１で暗号化して親機器７２に送り返し（”Ｒｅｓｐｏｎｓｅ”）、親機器７２の組み込み機能部７２１は暗号化した文字列を携帯機器７１に付随する公開鍵７１３２で復号し、復号した文字列と先に送ったランダムな文字列とが一致すれば携帯機器７１を通信してよい相手（つまり、携帯機器７１に付随する公開鍵７１３２と対をなす秘密鍵７１３１を所有するもの）であると認証する。

【０１８６】相互認証に成功した場合、携帯機器７１の組み込み機能部７１１および親機器７２の組み込み機能部７２１は、プログラム７１２の出所由来を表す公開鍵７１２２とプログラム７２２の出所由来を表す公開鍵７２２２とをお互いに相手に伝え、両公開鍵が一致するかどうかを判定し（ステップＳ７０５）、一致した場合に限り、プロセス７１２１０とプロセス７２２１０との間で通信を許可する（ステップＳ７０６）。

【０１８７】携帯機器７１と親機７２との相互認証に失敗した場合（ステップＳ７０４）、またはプログラム７１２の出所由来を表す公開鍵７１２２とプログラム７２２の出所由来を表す公開鍵７２２２とが一致しなかった場合（ステップＳ７０５）、携帯機器７１の組み込み機能部７１１および親機器７２の組み込み機能部７２１は、プロセス７１２０とプロセス７２２０との間の通信を不許可とする（ステップＳ７０７）。

【０１８８】第７の実施の形態によれば、携帯機器７１内のプログラム７１２および親機器７２内のプログラム７２２が、一致する公開鍵７１２２および７２２２を付随するプログラム７１２および７２２としか通信できず、任意の他のプログラムと通信できないため、携帯機器７１内のプログラム７１２および親機器７２内のプログラム７２２のもつ情報の、流通する範囲を出所由来を同じくするプログラムの範囲内に限ることができる。

【0189】また、携帯機器71内のプログラム712および親機器72内のプログラム722が、一致する公開鍵7122および72222を付随するプログラム712および722としか通信できず、任意の他のプログラムと通信できないため、携帯機器71内のプログラム712および親機器72内のプログラム722のもつ情報が、たとえプログラム712および722が暴走しても、出所由来を同じくするプログラムの範囲外に漏洩しない。

【0190】さらに、分散環境における通信範囲の制御についてのセキュリティ面での設計が容易になり、かつ自由度が変わらないことである。その理由は、分散環境におけるもっとも重要な問題の1つである通信時の情報漏洩について、製造元またはそれに類するものを同じくするプログラムの間でしか情報を流通させないために、設計時に情報の流通範囲を設計しなくても、悪意のある他者への漏洩や、プログラムのバグ，暴走による漏洩が起こらず、また、逆に1つのサービスにおいては、そのプロジェクトにかかわるもの全体である1つの製造元またはそれに類するものとみなすことで、情報の流通を行え、またその流通範囲で十分であるからである。

【0191】さらに、プログラム712、722が秘密鍵をもたなくても、携帯機器71および親機72は、相手内のプロセス7220、7120、の元となるプログラム722、712の認証が可能であることから、盗み見や改竄が可能な環境下にあるプログラム712、722を元にして動作する相手と通信を行う場合に、携帯機器71、親機器72がプログラム722、712の成りすましを防止しかつ認証を行うことができる。

【0192】（8） 第8の実施の形態

図15を参照すると、本発明の第8の実施の形態に係るプログラムID通信範囲制御方法および公開鍵毎通信路提供方法が適用された情報システムは、第7の実施の形態に係るプログラムID通信範囲制御方法が適用された情報システムにおいて、携帯機器81および親機器82が、さらに、通信装置815および825と、公開鍵毎にすべてのポート番号を割り振ることの出来る、つまり同じポート番号で公開鍵値毎に存在し得る仮想ソケット81511～8151iおよび82611～8251jと、ソケット81521～8152kおよび82521～82521とを含んで構成されている。なお、第7の実施の形態に係るプログラムID通信範囲制御方法が適用された情報システムにおける部分と対応する部分には、符号の先頭文字「7」を「8」に変更した符号を付して、それらの詳しい説明を省略する。

【0193】仮想ソケット81511～8151iおよび82611～8251jは、チャネル，パイプ等の他の通信路を仮想的にしたものでもよく、ソケット81521～8152kおよび82521～82521、チャネル，パイプ等の他の通信路であってもよい。

【0194】図16を参照すると、携帯機器81の組み込み機能部811および親機器82の組み込み機能部821の処理は、ハッシュ値確認ステップS801およびS802と、通信要求発生ステップS803と、相互認証ステップS804と、公開鍵一致判定ステップS805と、通信許可ステップS806と、通信不許可ステップS807とからなる。

【0195】次に、このように構成された第8の実施の形態に係るプログラムID通信範囲制御方法が適用された情報システムの動作について、図15および図16を参照して詳細に説明する。

【0196】ステップS801～ステップS805およびステップS807は、第7の実施の形態に係るプログラムID通信範囲制御方法におけるステップS701～ステップS705およびステップS707と同じである。

【0197】第7の実施の形態に係るプログラムID通信範囲制御方法が適用された情報システムの動作において、プロセス8120とプロセス8220との間で通信を許可するステップS806において、一致した場合に限り、通信装置815および825は、それぞれ、公開鍵8122および82222とプロセス81210およびプロセス82210が要求する仮想ソケットのポート番号の対に対し、組み込み機能部811と組み込み機能部821との間で使用しているソケットによる通信路に形成された仮想通信路の1つを割り当て、該仮想通信路によりプロセス81210とプロセス82210との間での通信を許可する。

【0198】（9） 第9の実施の形態

図17を参照すると、本発明の第9の実施の形態に係るプログラムID通信範囲制御方法が適用された情報システムは、プログラムの実行機能および通信機能を有する携帯機器91と、同じくプログラムの実行機能および通信機能を有する親機器92と、携帯機器91にインストールされ実行されるプログラム912と、親機器92にインストールされ実行されるプログラム922とから、その主要部が構成されている。

【0199】実行機能および通信機能は、Javaなどが想定される。

【0200】携帯機器91としては、携帯電話機（PHSを含む），携帯情報端末等が想定される。

【0201】親機器92としては、POS端末等が想定される。

【0202】携帯機器91と親機器92との間の通信機能に使用される通信方式は、エリクソン社等が提唱するBluetooth，無線LAN，PIAFS等の近距離無線通信技術で実現されるものとする。

【0203】携帯機器91は、信頼できる組み込み機能部911と、プログラム912を実行するプロセス9120と、携帯機器91に付随する秘密鍵9131および

公開鍵９１３２と、親機器９２に付随する公開鍵９２３２とを含んで構成されている。

【０２０４】プログラム９１２は、プログラム本体９１２１と、プログラム９１２の出所由来を表す公開鍵群９１２２１～９１２２ｎと、プログラム本体９１２１および公開鍵群９１２２１～９１２２ｎを組み合わせて作成されたデータをハッシュ関数でハッシングしたダイジェストを各公開鍵９１２２１～９１２２ｎと対をなす各秘密鍵（図示せず）で暗号化した署名群であるハッシュ値群９１２３１～９１２３ｎとを含んで構成されている。なお、プログラム９１２は、その出所（製造元等）および由来（バージョン等）において、プログラム本体９１２１，公開鍵群９１２２１～９１２２ｎ，およびハッシュ値群９１２３１～９１２３ｎが一体として作成されている。

【０２０５】親機器９２は、信頼できる組み込み機能部９２１と、プログラム９２２を実行するプロセス９２２０と、親機器９２に付随する秘密鍵９２３１および公開鍵９２３２と、携帯機器９１に付随する公開鍵９１３２とを含んで構成されている。

【０２０６】プログラム９２２は、プログラム本体９２２１と、プログラム９２２の出所由来を表す公開鍵群９２２２１～９２２２ｍ（ｍは２上の正整数。以下同様）と、プログラム本体９２２１および公開鍵群９２２２１～９２２２ｍにより構成されたデータをハッシュ関数でハッシングしたダイジェストを各公開鍵９２２２１～９２２２ｍと対をなす各秘密鍵（図示せず）で暗号化した署名群であるハッシュ値群９２２３１～９２２３ｍとを含んで構成されている。なお、プログラム９２２は、その出所（製造元等）および由来（バージョン等）において、プログラム本体９２２１，公開鍵群９２２２１～９２２２ｍ，およびハッシュ値群９２２３１～９２２３ｍが一体として作成されている。

【０２０７】図１８を参照すると、携帯機器９１の組み込み機能部９１１および親機器９２の組み込み機能部９２１の処理は、ハッシュ値確認ステップＳ９０１およびＳ９０２と、通信要求発生ステップＳ９０３と、相互認証ステップＳ９０４と、公開鍵一致判定ステップＳ９０５と、通信許可ステップＳ９０６と、通信不許可ステップＳ９０７とからなる。

【０２０８】次に、このように構成された第９の実施の形態に係るプログラムＩＤ通信範囲制御方法が適用された情報システムの動作について、図１７および図１８を参照して詳細に説明する。

【０２０９】まず、携帯機器９１は、組み込み機能部９１１により、各ハッシュ値９１２３１～９１２３ｎがプログラム本体９１２１および公開鍵群９１２２１～９１２２ｎと各公開鍵９１２２１～９１２２ｎと対をなす各秘密鍵とによって生成されたものであるかどうかを確認し、確認したハッシュ値に対応する公開鍵の集まりを得る（ステップＳ９０１）。詳しくは、組み込み機能部９１１は、各ハッシュ値９１２３１～９１２３ｎを各公開鍵９１２２１～９１２２ｎでそれぞれ復号してプログラム本体９１２１および公開鍵群９１２２１～９１２２ｎを組み合わせて作成されたデータをハッシングしたダイジェスト群を得る一方、プログラム本体９１２１および公開鍵群９１２２１～９１２２ｎを組み合わせて作成されたデータを既知のハッシュ関数でハッシングしてダイジェストを得、該ダイジェストとダイジェスト群の一つ一つが完全に一致するかどうかをそれぞれ検証することで、各ハッシュ値９１２３１～９１２３ｎがプログラム本体９１２１および公開鍵群９１２２１～９１２２ｎと各公開鍵９１２２１～９１２２ｎと対をなす各秘密鍵とによって生成されたものであることをそれぞれ確認し、確認したハッシュ値に対応する公開鍵の集まりを得る。すなわち、プログラム本体９１２１および公開鍵群９１２２１～９１２２ｎ中の少なくとも１つ以上の公開鍵が改竄されたものでなく、真正な出所由来をもつことを確認する。なお、この確認処理は、携帯機器９１にプログラム９１２が導入、たとえばダウンロードされたときなどに１回行われればよい。

【０２１０】また、携帯機器９２でも、組み込み機能部９２１が、各ハッシュ値９２２３１～９２２３ｎがプログラム本体９２２１および公開鍵群９２２２１～９２２２ｎと各公開鍵９２２２１～９２２２ｎと対をなす各秘密鍵（図示せず）とによって生成されたものであるかどうかを確認し、確認したハッシュ値に対応する公開鍵の集まりを得る（ステップＳ９０２）。詳しくは、組み込み機能部９２１は、各ハッシュ値９２２３１～９２２３ｍを公開鍵９２２２１～９２２２ｍでそれぞれ復号してプログラム本体９２２１および公開鍵群９２２２１～９２２２ｍを組み合わせて作成されたデータをハッシングした各ダイジェストを得る一方、プログラム本体９２２１および公開鍵群９２２２１～９２２２ｍを組み合わせて作成されたデータを既知のハッシュ関数でハッシングしたダイジェストを得、両各ダイジェストが完全に一致するかどうかをそれぞれ検証することで、各ハッシュ値９２２３１～９２２３ｎがプログラム本体９２２１および公開鍵群９２２２１～９２２２ｎと各公開鍵９２２２１～９２２２ｎと対をなす各秘密鍵（図示せず）とによって生成されたものであることをそれぞれ確認し、確認したハッシュ値に対応する公開鍵の集まりを得る。すなわち、プログラム本体９２２１および公開鍵群９２２２１～９２２２ｍ中の少なくとも１つ以上の公開鍵が改竄されたものでなく、真正な出所由来をもつことを確認する。なお、この確認処理は、親機器９２にプログラム９２２が導入、たとえばインストールされたときなどに１回行われればよい。

【０２１１】次に、携帯機器９１内のプログラム９１２を実行するプロセス９１２０と親機器９２内のプログラ

ム９２２を実行するプロセス９２２０とが通信をしようとして通信要求が発生した場合（ステップＳ９０３）、またはそれ以前に、まず、携帯機器９１の組み込み機能部９１１と親機器９２の組み込み機能部９２１との間で、携帯機器９１に付随する秘密鍵９１３１および公開鍵９１３２と、親機器９２に付随する秘密鍵９２３１および公開鍵９２３２とを用いた公開鍵方式により相互認証を行う（ステップＳ９０４）。

【０２１２】たとえば、親機器９２は、自らが通信してよい相手を示す公開鍵として保持する携帯機器９１に付随する公開鍵９１３２と、携帯機器９１が保持する携帯機器９１に付随する公開鍵９１１３２とが一致するかどうかを判定し、一致した場合に携帯機器９１の認証を行う。一方、携帯機器９１は、自らが通信してよい相手を示す公開鍵として保持する親機器９２に付随する公開鍵９２３２と、親機器９２が保持する親機器９２に付随する公開鍵９２１３２とが一致するかどうかを判定し、一致した場合に親機器９２の認証を行う。

【０２１３】また、ＲＳＡの公開鍵によるワン・タイム・パスワード方式を用いた場合、携帯機器９１の組み込み機能部９１１は親機器９２にランダムな文字列を送り（"Ｃｈａｌｌｅｎｇｅ"）、親機器９２の組み込み機能部９２１はその文字列を親機器９２に付随する秘密鍵９２３１で暗号化して携帯機器９１に送り返し（"Ｒｅｓｐｏｎｓｅ"）、携帯機器９１の組み込み機能部９１１は、暗号化した文字列を親機器９２に付随する公開鍵９２３２で復号し、復号した文字列と先に送ったランダムな文字列とが一致すれば、親機器９２を通信してよい相手（つまり、親機器９２に付随する公開鍵９２３２と対をなす秘密鍵９２３１を所有するもの）であると認証する。一方、親機器９２の組み込み機能部９２１は携帯機器９１にランダムな文字列を送り（"Ｃｈａｌｌｅｎｇｅ"）、携帯機器９１の組み込み機能部９１１はその文字列を携帯機器９１に付随する秘密鍵９１３１で暗号化して親機器９２に送り返し（"Ｒｅｓｐｏｎｓｅ"）、親機器９２の組み込み機能部９２１は暗号化した文字列を携帯機器９１に付随する公開鍵９１３２で復号し、復号した文字列と先に送ったランダムな文字列とが一致すれば、携帯機器９１を通信してよい相手（つまり、携帯機器９１に付随する公開鍵９１３２と対をなす秘密鍵９１３１を所有するもの）であると認証する。

【０２１４】相互認証に成功した場合、携帯機器９１の組み込み機能部９１１および親機器９２の組み込み機能部９２１は、ハッシュ値確認結果の公開鍵の集まりをお互いに相手に伝え、一致する公開鍵があるかどうかを判定し（ステップＳ９０５）、一致する公開鍵が１つ以上ある場合に限り、プロセス９１２１０とプロセス９２２１０との間で通信を許可する（ステップＳ９０６）。

【０２１５】ステップＳ９０４で携帯機器９１または親機９２の相互認証に失敗した場合、またはステップＳ９０５で一致する公開鍵が１つもなかった場合、携帯機器９１の組み込み機能部９１１および親機器９２の組み込み機能部９２１は、プロセス９１２０とプロセス９２２０との間の通信を不許可とする（ステップＳ９０７）。

【０２１６】なお、上記第９の実施の形態では、ステップＳ９０５で携帯機器９１によるハッシュ値確認結果の公開鍵の集まりと親機器９２によるハッシュ値確認結果の公開鍵の集まりとに一致する公開鍵が１つ以上含まれていればプログラム９１２および９２２が真正な出所由来をもつものであると判定したが、携帯機器９１によるハッシュ値確認結果の公開鍵の集まりと親機器９２によるハッシュ値確認結果の公開鍵の集まりとの公開鍵がすべて一致したときにのみ、プロセス９１２１０とプロセス９２２１０との間で通信を許可するようにすることもできる。

【０２１７】第９の実施の形態によれば、プログラム９１２および９２２が該プログラム９１２および９２２の出所由来を表す公開鍵群９１２２１～９１２２ｎおよび９２２２１～９２２２ｎをもつことを許す場合はプログラム本体９１２１および９２２１とともに保持する公開鍵群９１２２１～９１２２ｎおよび９２２２１～９２２２ｎに対して署名群であるハッシュ値群９１２３１～９１２３ｎおよび９２２３１～９２２３ｎを付すことから、プログラム５１２および５２２の成りすましを防止することができる。

【０２１８】

【発明の効果】第１の効果は、外部装置が、盗み見や改竄が可能な環境下にあるプログラムを元にし動作する装置と通信を行う場合に、成りすましを防止しかつ通信相手のプログラムの認証を行うことができることである。その理由は、プログラムが秘密鍵をもたないで認証が可能だからである。

【０２１９】第２の効果は、プログラムが成りすましを防止しかつ複数の出所由来を表す公開鍵をもつことを許すことができることである。その理由は、複数の出所由来を表す公開鍵をもつことを許す場合は、プログラム本体とともに保持する公開鍵群に対し署名するからである。

【０２２０】第３の効果は、悪意のプログラムに対しセキュリティを保てることである。その理由は、プログラムの出所由来を表すＩＤ、つまりプログラムの製造元やバージョンに類する情報を元にしたアクセス制御により通信を行うからである。

【０２２１】第４の効果は、ユーザ管理のような集中管理システムを必要としない分散環境下での通信による処理についてのセキュリティを保てることである。その理由は、プログラムの出所由来を表すＩＤ、つまりプログラムの製造元やバージョンに類する情報を元にしたアクセス制御により通信を行うため、悪意のプログラムに対しセキュリティを保てるからである。

【0222】第5の効果は、プログラム実行・通信装置内のプログラムのもつ情報の、流通する範囲が出所由来を同じくするプログラムの範囲内に限られることである。その理由は、プログラム実行・通信装置内のプログラムが、一致する出所由来を表すＩＤを有するプログラムとしか通信できず、任意の他のプログラムと通信できないためである。

【0223】第6の効果は、プログラム実行・通信装置内のプログラムのもつ情報が、たとえプログラムが暴走しても、出所由来を同じくするプログラムの範囲外に漏洩しないことである。その理由は、プログラム実行・通信装置内のプログラムが、一致する出所由来を表すＩＤを有するプログラムとしか通信できず、任意の他のプログラムと通信できないためである。

【0224】第7の効果は、プログラム実行・通信装置内のプログラムのもつ情報の、流通する範囲が、出所由来を同じくするプログラムの範囲内に限られることである。その理由は、プログラム実行・通信装置内のプログラムが、一致する出所由来を表すＩＤを公開鍵とすることにより、同じ秘密鍵を保持するものにより提供されたプログラムの間でしか、通信ができないからである。

【0225】第8の効果は、分散環境における通信範囲の制御についてのセキュリティ面での設計が容易になり、かつ自由度が変わらないことである。その理由は、分散環境におけるもっとも重要な問題の１つである通信時の情報漏洩について、出所由来を同じくするプログラムの間でしか情報を流通させないために、設計時に情報の流通範囲を設計しなくても、悪意のある他者への漏洩や、プログラムのバグ、暴走による漏洩が起こらず、また、逆に１つのサービスにおいては、そのプロジェクトにかかわるもの全体である１つの製造元またはそれに類するものとみなすことで、情報の流通を行え、またその流通範囲で十分であるからである。

【0226】第9の効果は、悪意のプログラムに対しセキュリティを保てることである。その理由は、プログラムの出所由来を表すＩＤ、つまりプログラムの製造元やバージョンに類する情報を元に通信可否を行うからである。

【0227】第１０の効果は、ユーザ管理のような集中管理システムを必要としない分散環境下での通信による処理についてのセキュリティを保てることである。その理由は、プログラムの出所由来を表すＩＤ、つまりプログラムの製造元やバージョンに類する情報を元に通信可否を行うため、悪意のプログラムに対しセキュリティを保てるからである。

【0228】第１１の効果は、公開鍵別の通信を行う場合に、通信路に関するシステム設計が容易であることである。その理由は、どの通信路がどの公開鍵用で占有されるかが予め限定されているからである。

【図面の簡単な説明】

【図１】本発明の第１の実施の形態に係る秘密鍵なしプログラム認証方法が適用された情報システムの構成を示すブロック図である。

【図２】第１の実施の形態に係る秘密鍵なしプログラム認証方法が適用された情報システムの処理を示す流れ図である。

【図３】本発明の第２の実施の形態に係る秘密鍵なしプログラム認証方法が適用された情報システムの構成を示すブロック図である。

【図４】第２の実施の形態に係る秘密鍵なしプログラム認証方法が適用された情報システムの処理を示す流れ図である。

【図５】本発明の第３の実施の形態に係るプログラムＩＤ通信処理制御方法が適用された情報システムの構成を示すブロック図である。

【図６】第３の実施の形態に係るプログラムＩＤ通信処理制御方法が適用された情報システムの処理を示す流れ図である。

【図７】本発明の第４の実施の形態に係るプログラムＩＤ通信処理制御方法が適用された情報システムの構成を示すブロック図である。

【図８】第４の実施の形態に係るプログラムＩＤ通信処理制御方法が適用された情報システムの処理を示す流れ図である。

【図９】本発明の第５の実施の形態に係るプログラムＩＤ通信処理制御方法が適用された情報システムの構成を示すブロック図である。

【図１０】第５の実施の形態に係るプログラムＩＤ通信処理制御方法が適用された情報システムの処理を示す流れ図である。

【図１１】本発明の第６の実施の形態に係るプログラムＩＤ通信範囲制御方法が適用された情報システムの構成を示すブロック図である。

【図１２】第６の実施の形態に係るプログラムＩＤ通信範囲制御方法が適用された情報システムの処理を示す流れ図である。

【図１３】本発明の第７の実施の形態に係るプログラムＩＤ通信範囲制御方法が適用された情報システムの構成を示すブロック図である。

【図１４】第７の実施の形態に係るプログラムＩＤ通信範囲制御方法が適用された情報システムの処理を示す流れ図である。

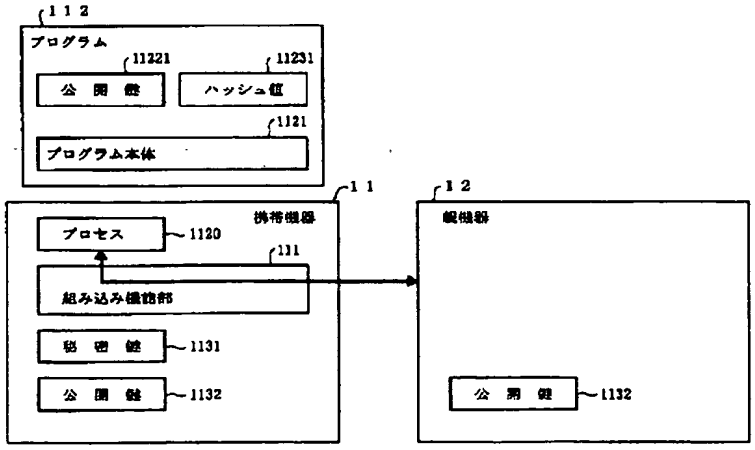
【図１５】本発明の第８の実施の形態に係るプログラムＩＤ通信範囲制御方法が適用された情報システムの構成を示すブロック図である。

【図１６】第８の実施の形態に係るプログラムＩＤ通信範囲制御方法が適用された情報システムの処理を示す流れ図である。

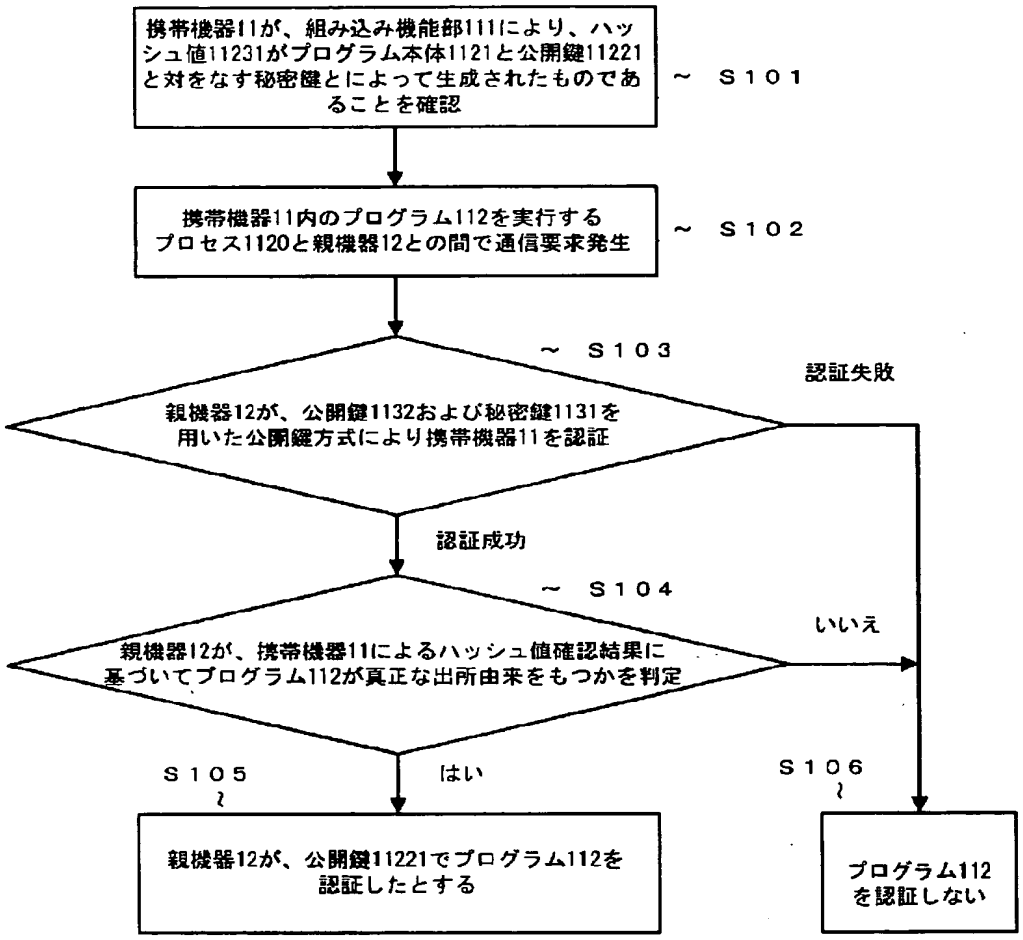
【図１７】本発明の第９の実施の形態に係るプログラムＩＤ通信範囲制御方法が適用された情報システムの構成

を示すブロック図である。
【図１８】第9の実施の形態に係るプログラムＩＤ通信範囲制御方法が適用された情報システムの処理を示す流れ図である。
【図１９】従来の情報システムの構成の一例を説明するブロック図である。
【図２０】従来の情報システムの構成の他の例を説明するブロック図である。
【図２１】従来の情報システムの構成の別の例を説明するブロック図である。
【符号の説明】
１１，…，９１　携帯機器
１２，…，９２　親機器
１１１，…，９１１　組み込み機能部
１１２，…，９１２　プログラム
１１２０，…，９１２０　プロセス
１１２１，…，９１２１　プログラム本体
１１２２１～１１２２ｎ，…，９１２２１～９１２２ｎ　公開鍵
１１２３１～１１２３ｎ，…，９１２３１～９１２３ｎ　ハッシュ値
１１２４１～１１２４ｎ，…，９１２４１～９１２４ｎ　秘密鍵
１１３１，…，９１３１　秘密鍵
１１３２，…，９１３２　公開鍵
８１５１１～８１５１ｉ，８２５１１～８２５１ｊ　仮想ソケット
８１５２１～８１５２ｋ，８２５２１～８２５２ｌ　ソケット
Ｓ１０１，Ｓ２０１，Ｓ４０１，Ｓ５０１，Ｓ７０１，Ｓ７０２，Ｓ８０１，Ｓ８０２，Ｓ９０１，Ｓ９０２　ハッシュ値確認ステップ
Ｓ１０２，Ｓ２０２，Ｓ３０１，Ｓ４０２，Ｓ５０２，Ｓ６０１，Ｓ７０３，Ｓ８０３，Ｓ９０３　通信要求発生ステップ
Ｓ１０３，Ｓ２０３，Ｓ４０３，Ｓ５０３　携帯機器認証ステップ
Ｓ１０４，Ｓ２０４，Ｓ４０４，Ｓ５０４　プログラム出所由来判定ステップ
Ｓ１０５，Ｓ２０５，Ｓ３０３　プログラム認証ステップ
Ｓ１０６，Ｓ２０６　プログラム不認証ステップ
Ｓ３０２，Ｓ６０２　公開鍵獲得ステップ
Ｓ３０４，Ｓ４０５，Ｓ５０５　通信・処理ステップ
Ｓ３０５，Ｓ４０６，Ｓ５０６　通信・処理なしステップ
Ｓ６０３，Ｓ７０４　相互認証ステップ
Ｓ６０４　公開鍵比較ステップ
Ｓ６０５　相互認証・公開鍵一致判定ステップ
Ｓ６０６，Ｓ７０６，Ｓ８０６，Ｓ９０６　通信許可ステップ
Ｓ６０７，Ｓ７０７，Ｓ８０７，Ｓ９０７　通信不許可ステップ
Ｓ７０５，Ｓ８０５，Ｓ９０５　公開鍵一致判定ステップ
Ｓ８０４，Ｓ９０４　相互認証ステップ

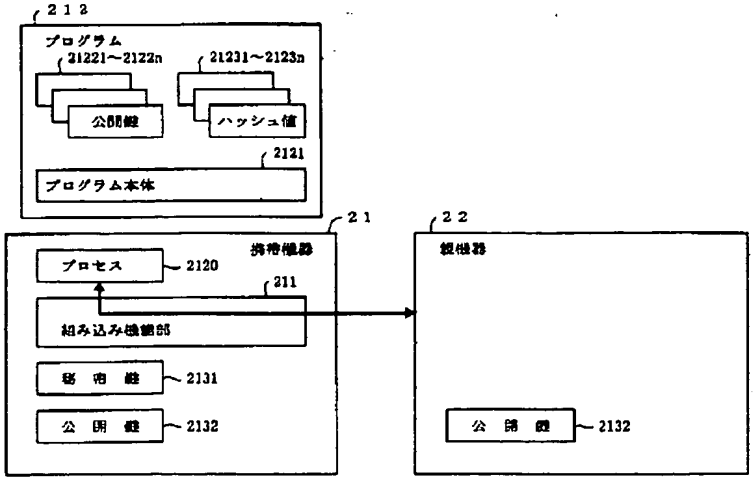
【図１】



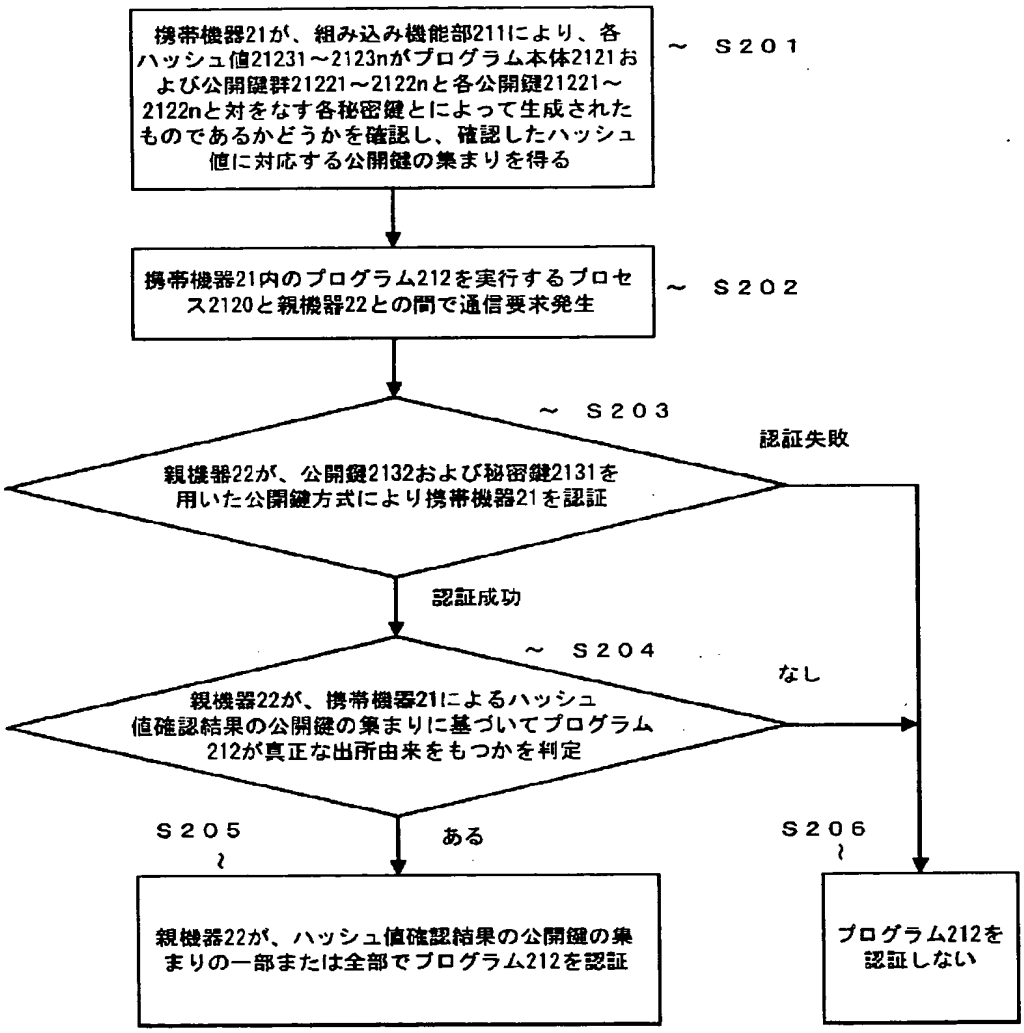
【図２】


携帯機器11が、組み込み機能部111により、ハッシュ値11231がプログラム本体1121と公開鍵11221と対をなす秘密鍵とによって生成されたものであることを確認
～ Ｓ１０１
携帯機器11内のプログラム112を実行するプロセス1120と親機器12との間で通信要求発生
～ Ｓ１０２
～ Ｓ１０３
親機器12が、公開鍵1132および秘密鍵1131を用いた公開鍵方式により携帯機器11を認証
認証失敗
認証成功
～ Ｓ１０４
親機器12が、携帯機器11によるハッシュ値確認結果に基づいてプログラム112が真正な出所由来をもつかを判定
いいえ
Ｓ１０５
はい
Ｓ１０６
親機器12が、公開鍵11221でプログラム112を認証したとする
プログラム112を認証しない

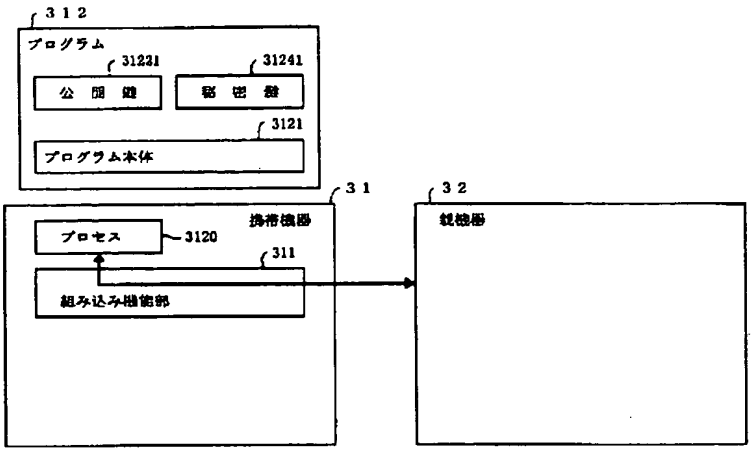
【図３】


212
プログラム
21221～2122n
21231～2123n
公開鍵
ハッシュ値
2121
プログラム本体
21
携帯機器
プロセス
2120
211
組み込み機能部
秘密鍵
2131
公開鍵
2132
22
親機器
公開鍵
2132

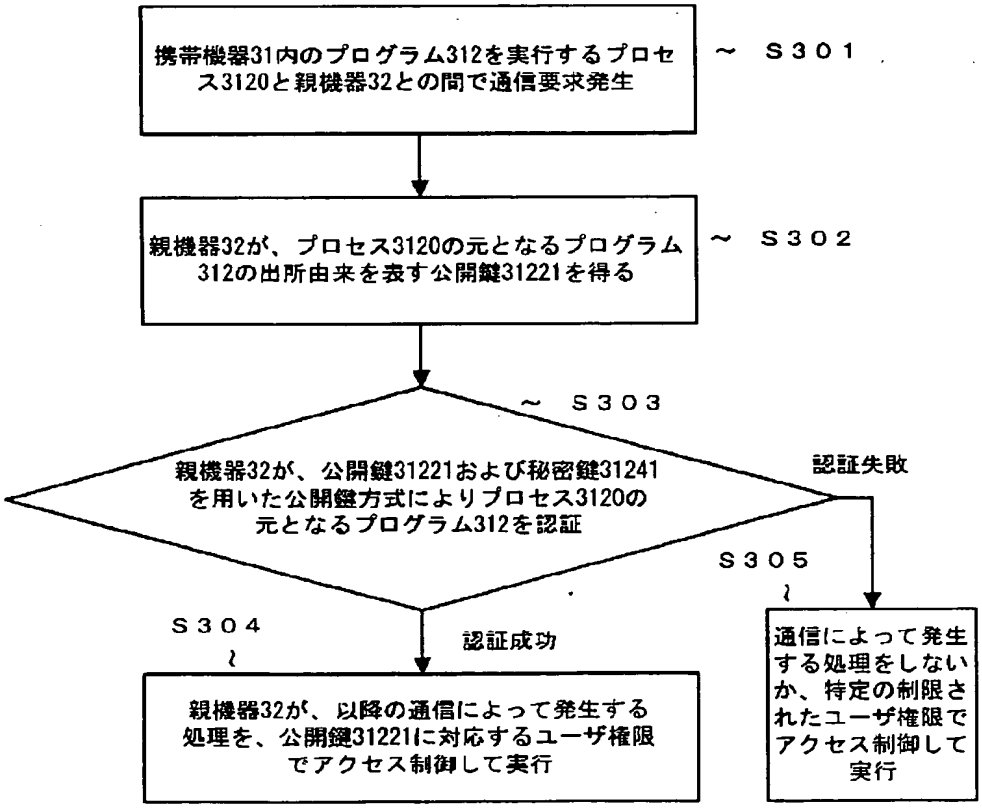
【図4】


携帯機器21が、組み込み機能部211により、各ハッシュ値21231～2123nがプログラム本体2121および公開鍵群21221～2122nと各公開鍵21221～2122nと対をなす各秘密鍵とによって生成されたものであるかどうかを確認し、確認したハッシュ値に対応する公開鍵の集まりを得る
～ S201
携帯機器21内のプログラム212を実行するプロセス2120と親機器22との間で通信要求発生
～ S202
～ S203
親機器22が、公開鍵2132および秘密鍵2131を用いた公開鍵方式により携帯機器21を認証
認証失敗
認証成功
～ S204
親機器22が、携帯機器21によるハッシュ値確認結果の公開鍵の集まりに基づいてプログラム212が真正な出所由来をもつかを判定
なし
ある
S205
S206
親機器22が、ハッシュ値確認結果の公開鍵の集まりの一部または全部でプログラム212を認証
プログラム212を認証しない

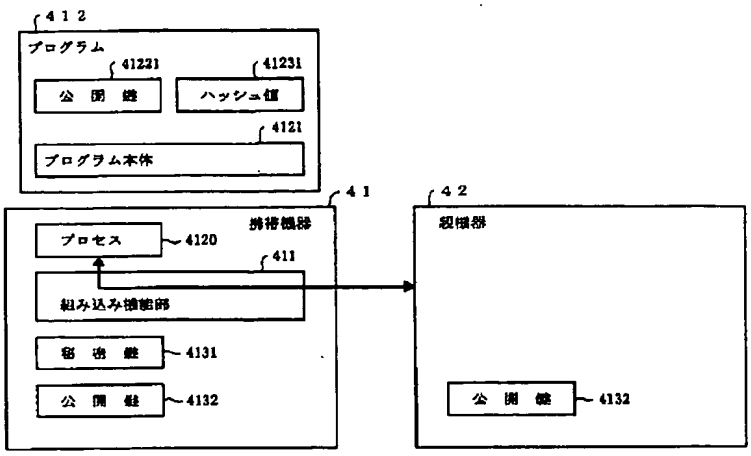
【図5】


312
プログラム
31231
公開鍵
31241
秘密鍵
3121
プログラム本体
31
携帯機器
プロセス
3120
311
組み込み機能部
32
親機器

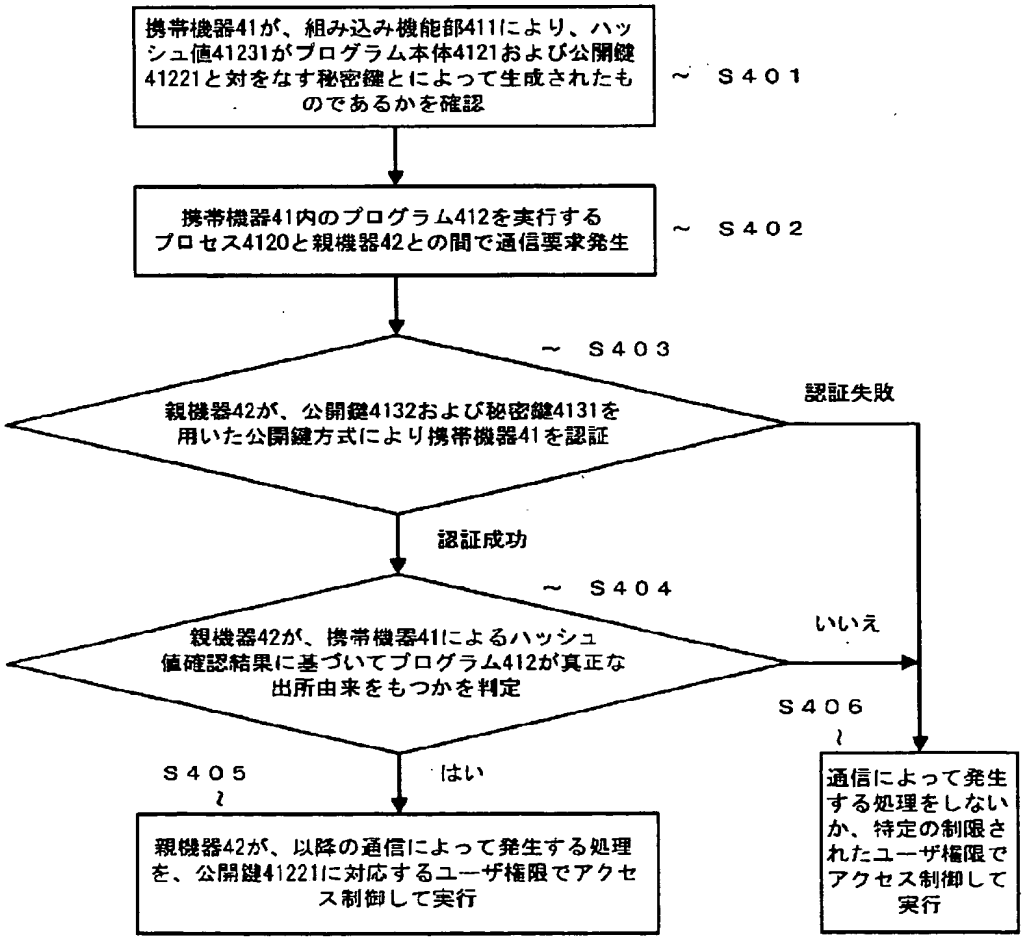
【図6】


携帯機器31内のプログラム312を実行するプロセス3120と親機器32との間で通信要求発生
～ S301
親機器32が、プロセス3120の元となるプログラム312の出所由来を表す公開鍵31221を得る
～ S302
～ S303
親機器32が、公開鍵31221および秘密鍵31241を用いた公開鍵方式によりプロセス3120の元となるプログラム312を認証
認証失敗
S305
通信によって発生する処理をしないか、特定の制限されたユーザ権限でアクセス制御して実行
S304
認証成功
親機器32が、以降の通信によって発生する処理を、公開鍵31221に対応するユーザ権限でアクセス制御して実行

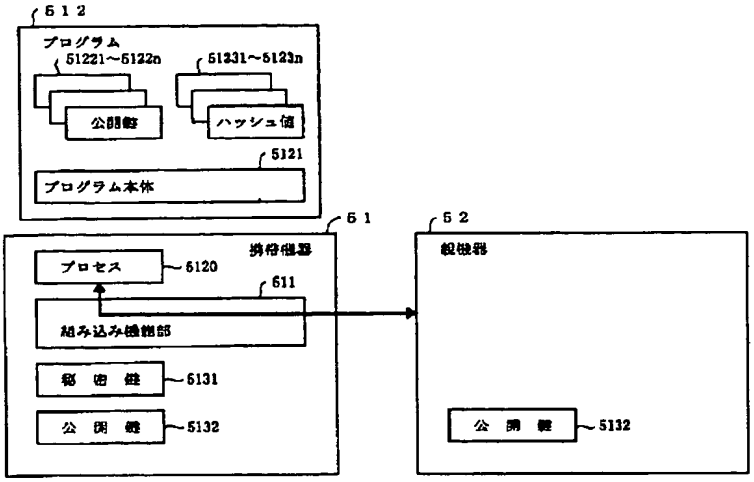
【図7】


412
プログラム
41221
41231
公開鍵
ハッシュ値
4121
プログラム本体
41
携帯機器
42
親機器
プロセス
4120
411
組み込み機能部
秘密鍵
4131
公開鍵
4132
公開鍵
4132

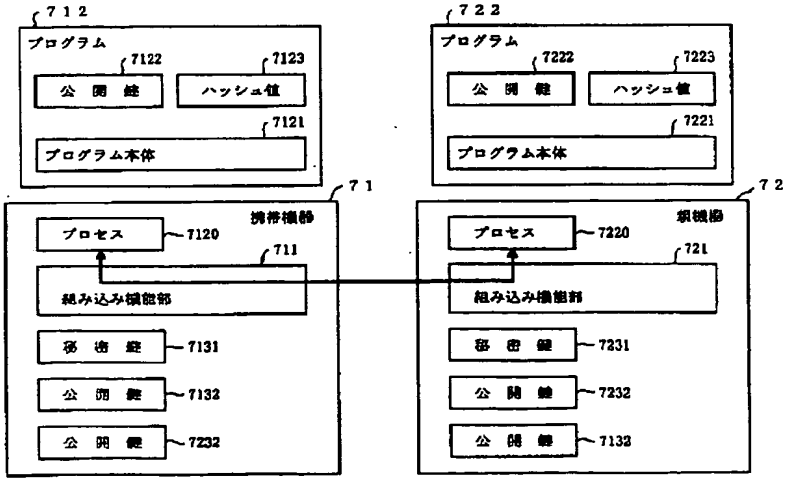
【図8】


携帯機器41が、組み込み機能部411により、ハッシュ値41231がプログラム本体4121および公開鍵41221と対をなす秘密鍵とによって生成されたものであるかを確認
～ S401
携帯機器41内のプログラム412を実行するプロセス4120と親機器42との間で通信要求発生
～ S402
～ S403
親機器42が、公開鍵4132および秘密鍵4131を用いた公開鍵方式により携帯機器41を認証
認証失敗
認証成功
～ S404
親機器42が、携帯機器41によるハッシュ値確認結果に基づいてプログラム412が真正な出所由来をもつかを判定
いいえ
S406
はい
S405
親機器42が、以降の通信によって発生する処理を、公開鍵41221に対応するユーザ権限でアクセス制御して実行
通信によって発生する処理をしないか、特定の制限されたユーザ権限でアクセス制御して実行

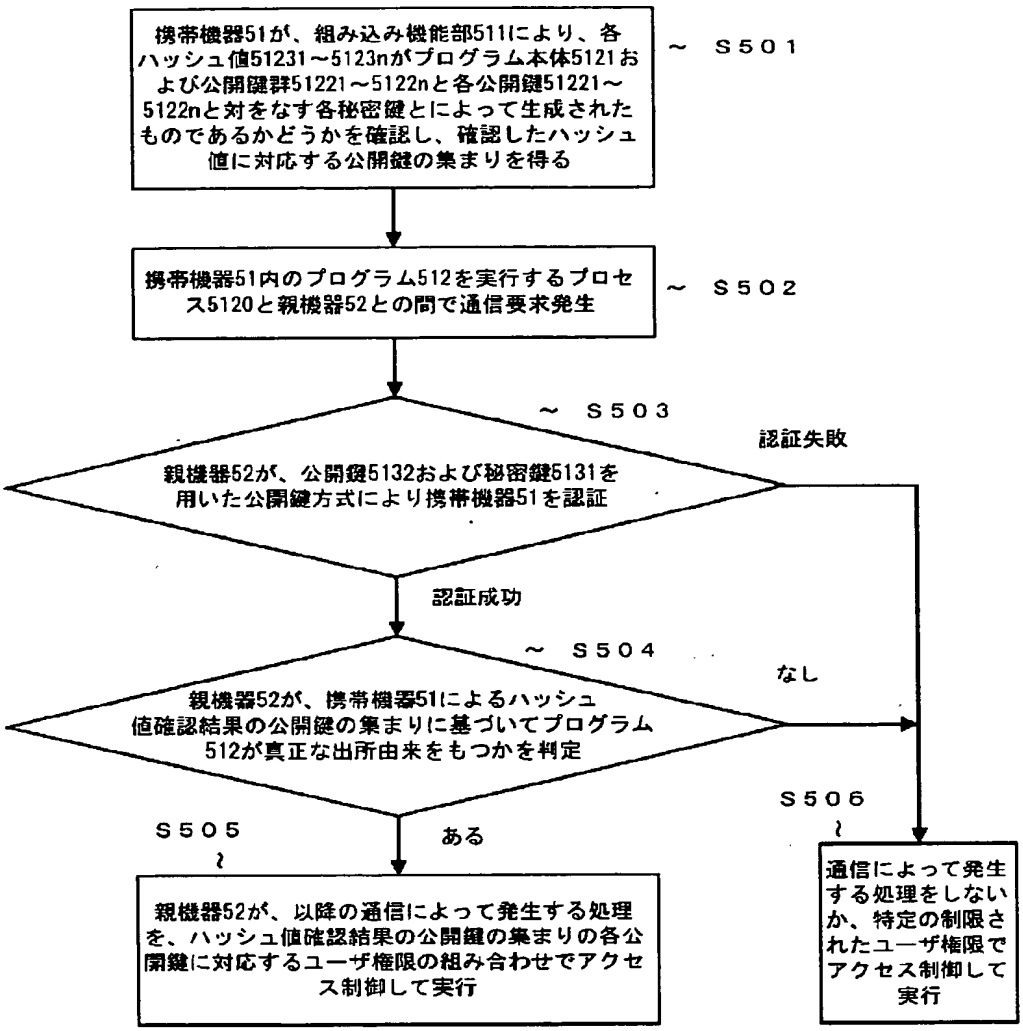
【図9】


512
プログラム
51221～5122n
51231～5123n
公開鍵
ハッシュ値
5121
プログラム本体
51
携帯機器
プロセス
5120
611
組み込み機能部
秘密鍵
5131
公開鍵
5132
52
般機器
公開鍵
5132

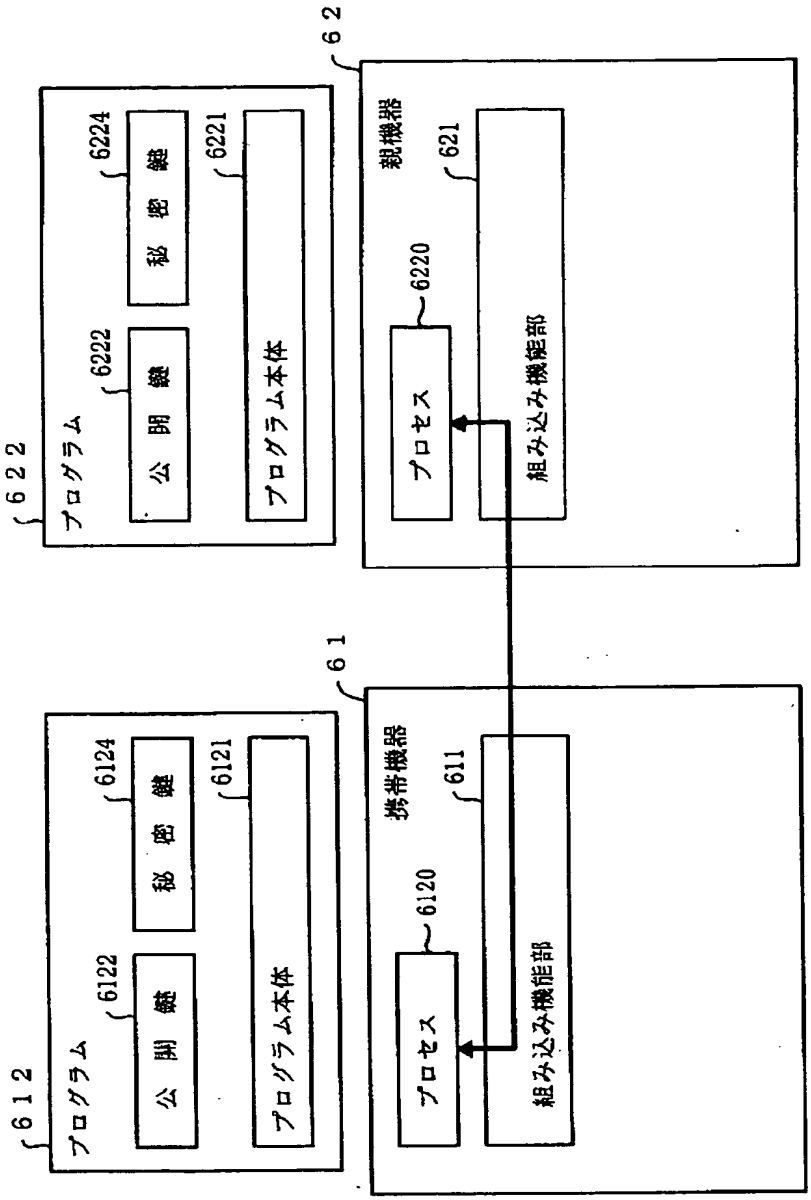
【図13】


712
プログラム
7122
7123
公開鍵
ハッシュ値
7121
プログラム本体
722
プログラム
7222
7223
公開鍵
ハッシュ値
7221
プログラム本体
71
携帯機器
プロセス
7120
711
組み込み機能部
秘密鍵
7131
公開鍵
7132
公開鍵
7232
72
般機器
プロセス
7220
721
組み込み機能部
秘密鍵
7231
公開鍵
7232
公開鍵
7132

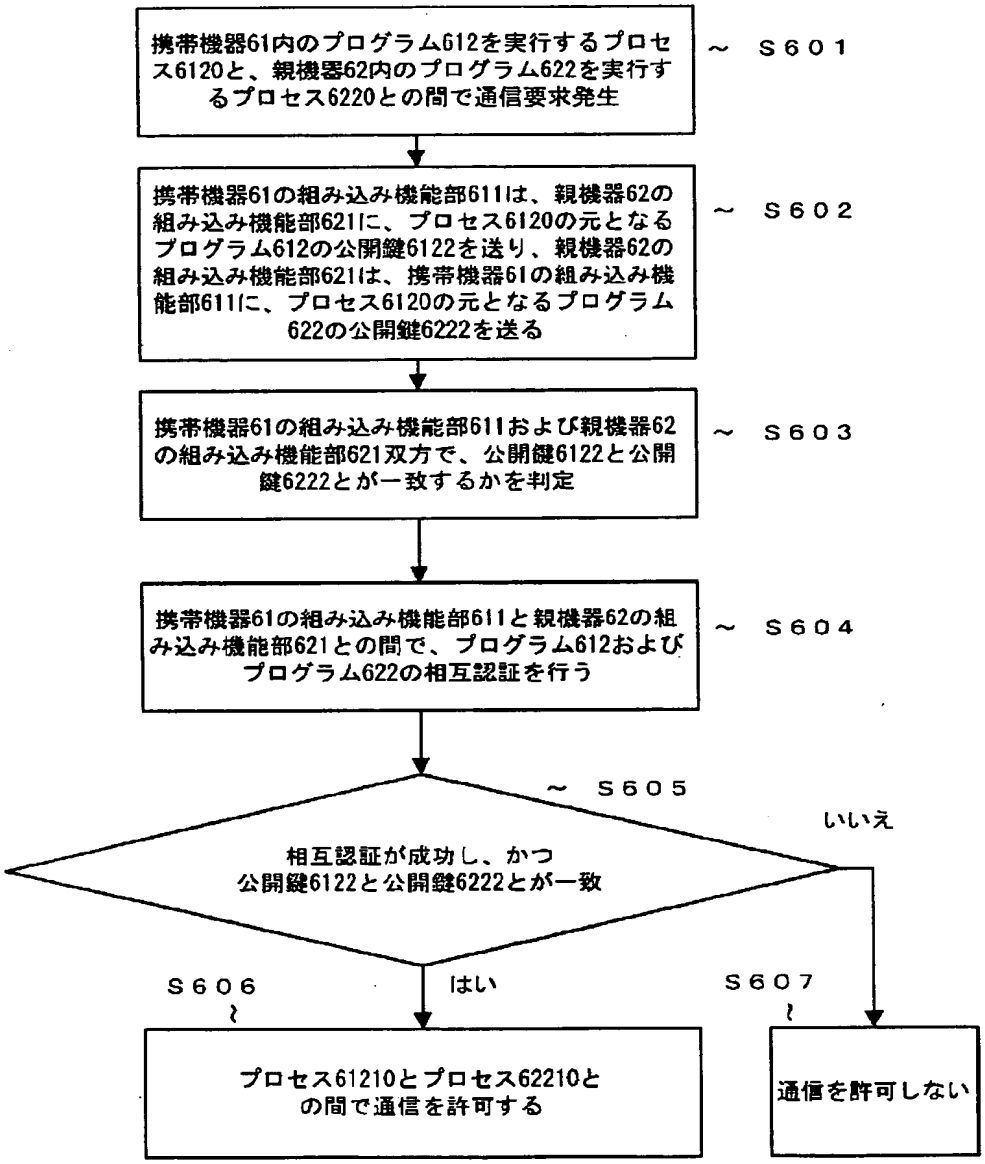
【図10】


携帯機器51が、組み込み機能部511により、各ハッシュ値51231～5123nがプログラム本体5121および公開鍵群51221～5122nと各公開鍵51221～5122nと対をなす各秘密鍵とによって生成されたものであるかどうかを確認し、確認したハッシュ値に対応する公開鍵の集まりを得る
～ S501
携帯機器51内のプログラム512を実行するプロセス5120と親機器52との間で通信要求発生
～ S502
～ S503
親機器52が、公開鍵5132および秘密鍵5131を用いた公開鍵方式により携帯機器51を認証
認証失敗
認証成功
～ S504
親機器52が、携帯機器51によるハッシュ値確認結果の公開鍵の集まりに基づいてプログラム512が真正な出所由来をもつかを判定
なし
ある
S505
親機器52が、以降の通信によって発生する処理を、ハッシュ値確認結果の公開鍵の集まりの各公開鍵に対応するユーザ権限の組み合わせでアクセス制御して実行
S506
通信によって発生する処理をしないか、特定の制限されたユーザ権限でアクセス制御して実行

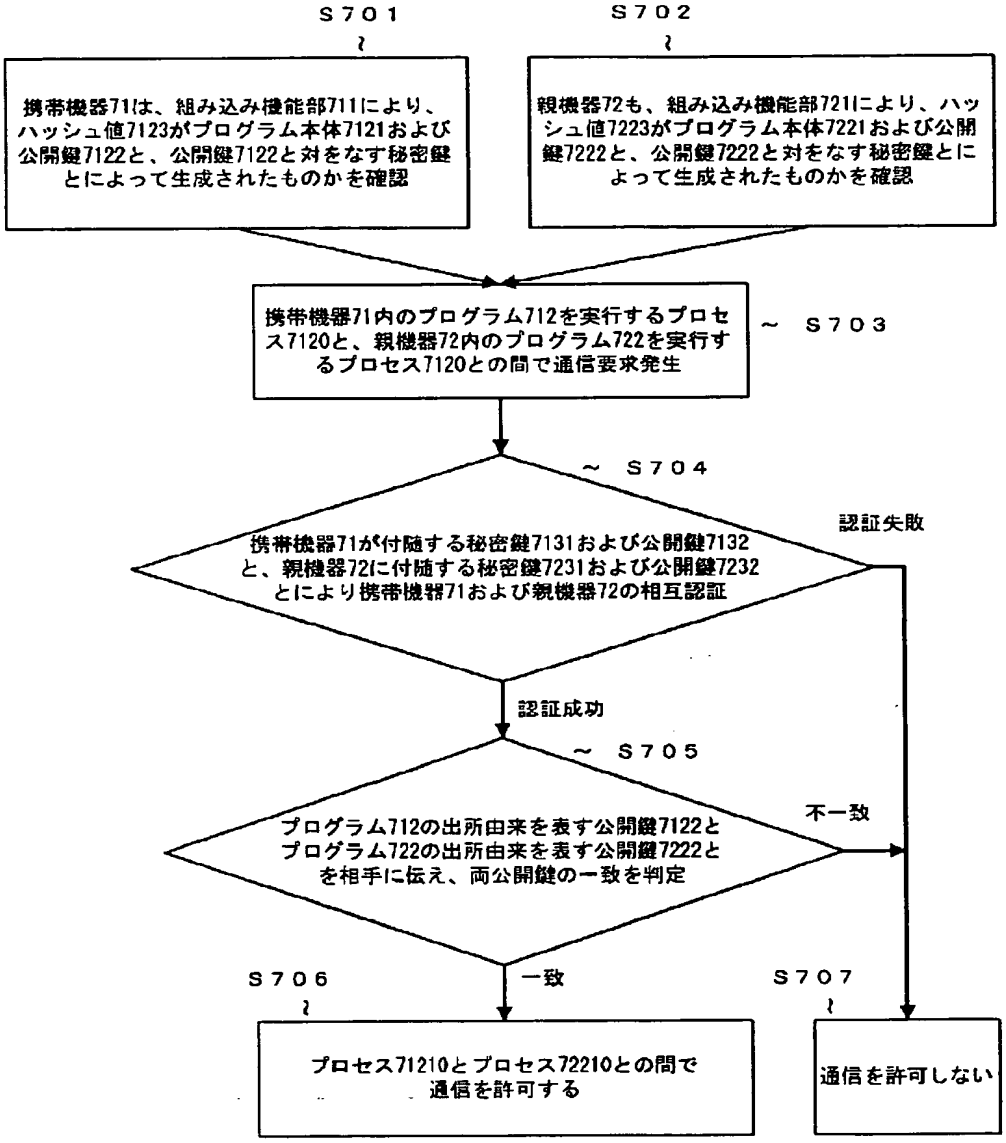
【図11】


62
親機器
621
組み込み機能部
6220
プロセス
6224
秘密鍵
6221
プログラム本体
6222
公開鍵
622
プログラム
61
携帯機器
611
組み込み機能部
6120
プロセス
6124
秘密鍵
6121
プログラム本体
6122
公開鍵
612
プログラム

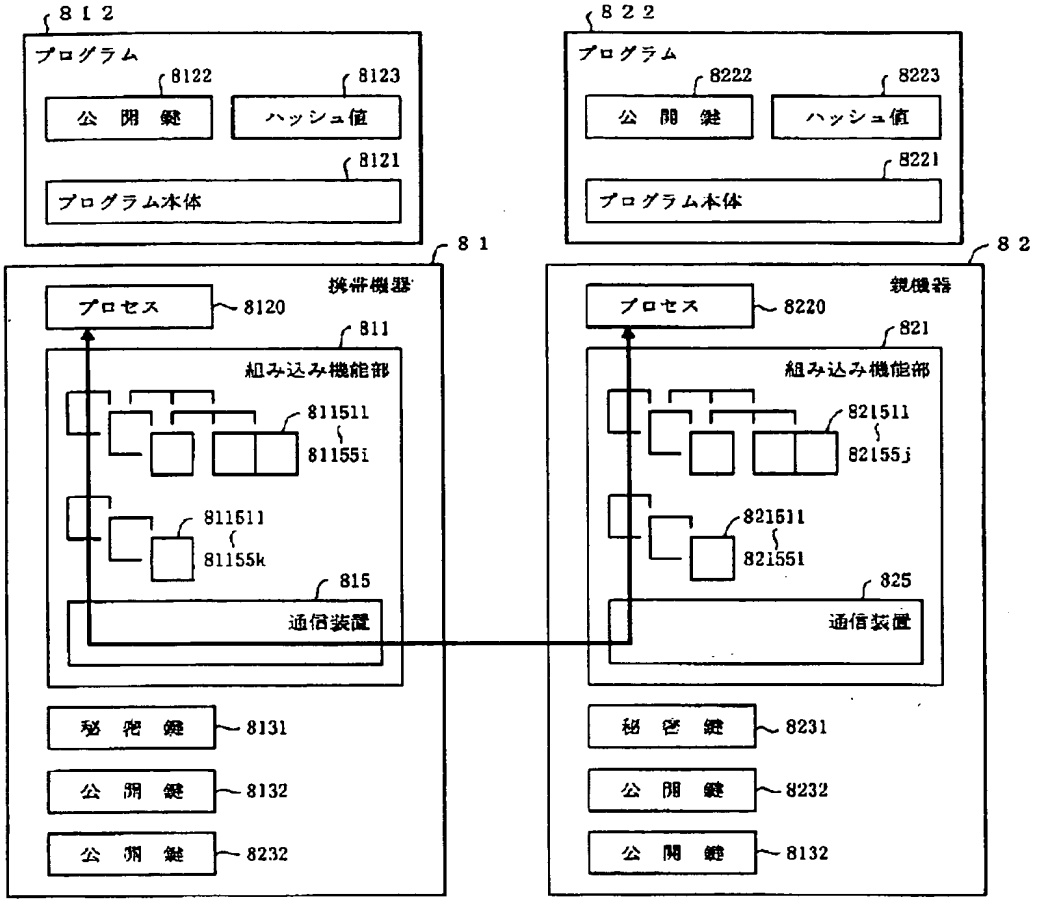
【図12】


携帯機器61内のプログラム612を実行するプロセス6120と、親機器62内のプログラム622を実行するプロセス6220との間で通信要求発生
～ S601
携帯機器61の組み込み機能部611は、親機器62の組み込み機能部621に、プロセス6120の元となるプログラム612の公開鍵6122を送り、親機器62の組み込み機能部621は、携帯機器61の組み込み機能部611に、プロセス6120の元となるプログラム622の公開鍵6222を送る
～ S602
携帯機器61の組み込み機能部611および親機器62の組み込み機能部621双方で、公開鍵6122と公開鍵6222とが一致するかを判定
～ S603
携帯機器61の組み込み機能部611と親機器62の組み込み機能部621との間で、プログラム612およびプログラム622の相互認証を行う
～ S604
～ S605
相互認証が成功し、かつ
公開鍵6122と公開鍵6222とが一致
いいえ
はい
S606
S607
プロセス61210とプロセス62210との間で通信を許可する
通信を許可しない

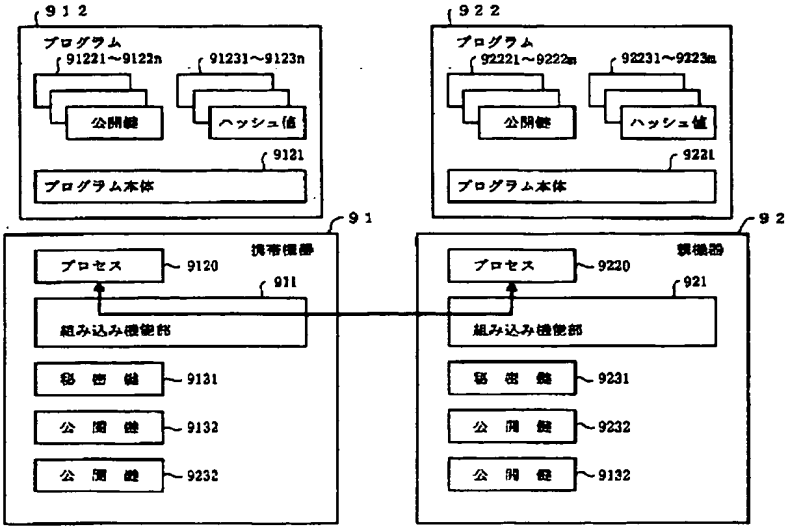
【図14】


S701
携帯機器71は、組み込み機能部711により、ハッシュ値7123がプログラム本体7121および公開鍵7122と、公開鍵7122と対をなす秘密鍵とによって生成されたものかを確認
S702
親機器72も、組み込み機能部721により、ハッシュ値7223がプログラム本体7221および公開鍵7222と、公開鍵7222と対をなす秘密鍵とによって生成されたものかを確認
携帯機器71内のプログラム712を実行するプロセス7120と、親機器72内のプログラム722を実行するプロセス7120との間で通信要求発生
S703
S704
携帯機器71が付随する秘密鍵7131および公開鍵7132と、親機器72に付随する秘密鍵7231および公開鍵7232とにより携帯機器71および親機器72の相互認証
認証失敗
認証成功
S705
プログラム712の出所由来を表す公開鍵7122とプログラム722の出所由来を表す公開鍵7222とを相手に伝え、両公開鍵の一致を判定
不一致
一致
S706
プロセス71210とプロセス72210との間で通信を許可する
S707
通信を許可しない

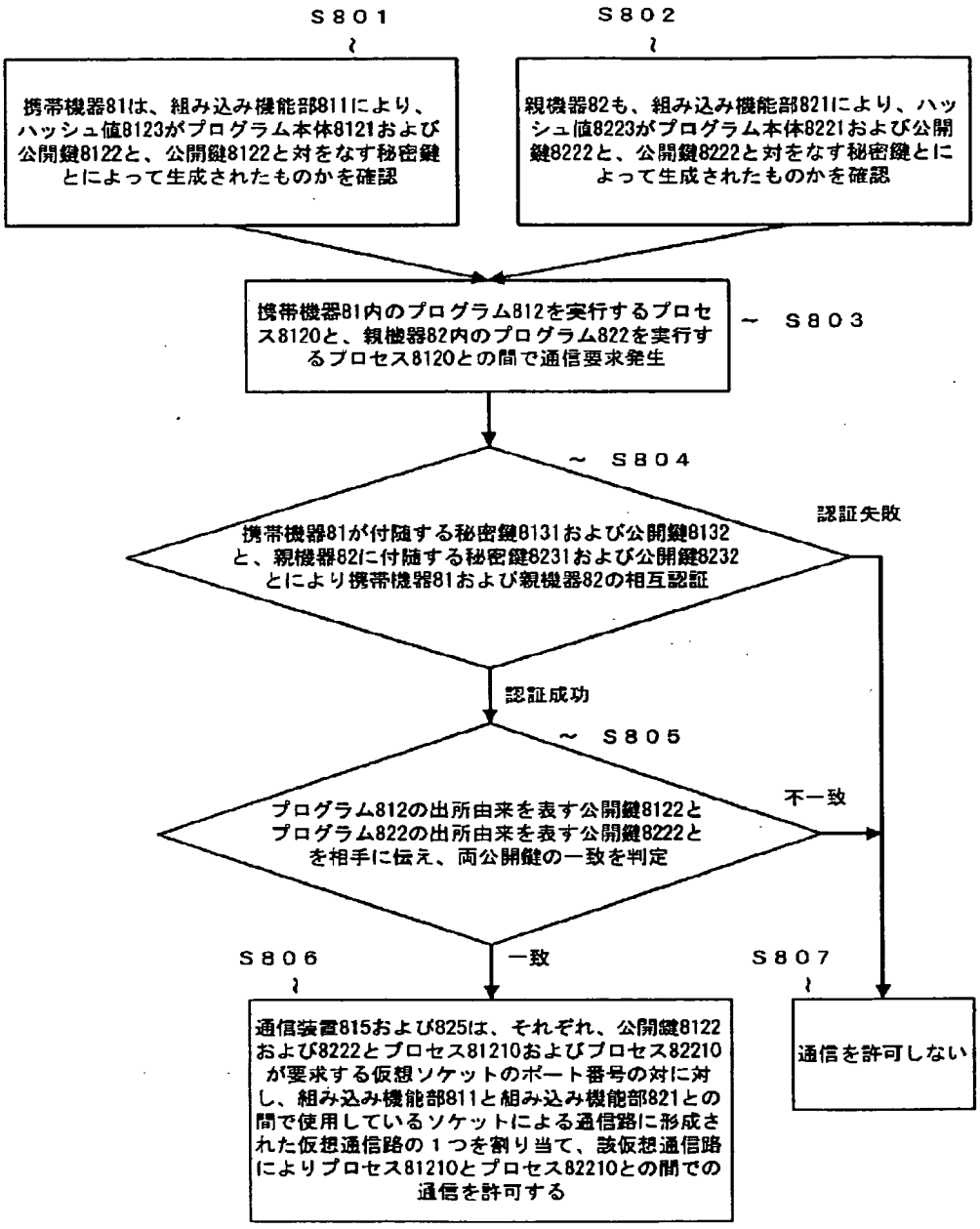
【図15】


812
プログラム
8122
公開鍵
8123
ハッシュ値
8121
プログラム本体
822
プログラム
8222
公開鍵
8223
ハッシュ値
8221
プログラム本体
81
携帯機器
プロセス
8120
811
組み込み機能部
811511
81155i
811611
81155k
815
通信装置
秘密鍵
8131
公開鍵
8132
公開鍵
8232
82
親機器
プロセス
8220
821
組み込み機能部
821511
82155j
821611
821551
825
通信装置
秘密鍵
8231
公開鍵
8232
公開鍵
8132

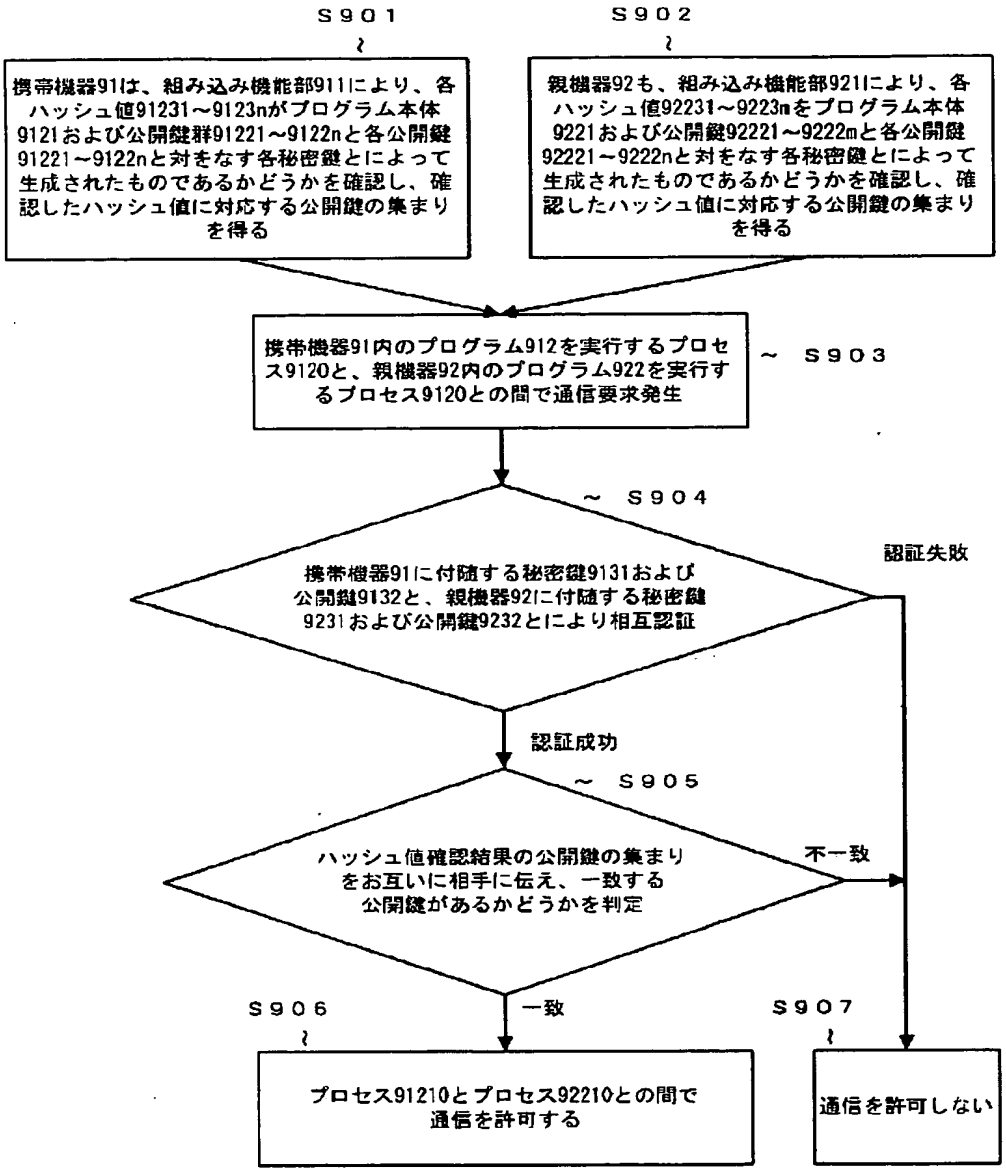
【図17】


912
プログラム
91221～9122n
91231～9123n
公開鍵
ハッシュ値
9121
プログラム本体
922
プログラム
92221～9222n
92231～9223n
公開鍵
ハッシュ値
9221
プログラム本体
91
携帯機器
プロセス
9120
911
組み込み機能部
秘密鍵
9131
公開鍵
9132
公開鍵
9232
92
親機器
プロセス
9220
921
組み込み機能部
秘密鍵
9231
公開鍵
9232
公開鍵
9132

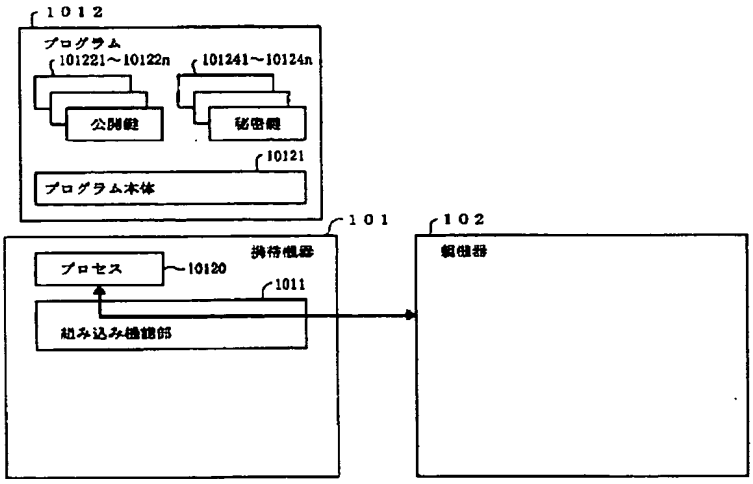
【図16】


S801
携帯機器81は、組み込み機能部811により、ハッシュ値8123がプログラム本体8121および公開鍵8122と、公開鍵8122と対をなす秘密鍵とによって生成されたものかを確認
S802
親機器82も、組み込み機能部821により、ハッシュ値8223がプログラム本体8221および公開鍵8222と、公開鍵8222と対をなす秘密鍵とによって生成されたものかを確認
携帯機器81内のプログラム812を実行するプロセス8120と、親機器82内のプログラム822を実行するプロセス8120との間で通信要求発生
S803
S804
携帯機器81が付随する秘密鍵8131および公開鍵8132と、親機器82に付随する秘密鍵8231および公開鍵8232とにより携帯機器81および親機器82の相互認証
認証失敗
認証成功
S805
プログラム812の出所由来を表す公開鍵8122とプログラム822の出所由来を表す公開鍵8222とを相手に伝え、両公開鍵の一致を判定
不一致
一致
S806
通信装置815および825は、それぞれ、公開鍵8122および8222とプロセス81210およびプロセス82210が要求する仮想ソケットのポート番号の対に対し、組み込み機能部811と組み込み機能部821との間で使用しているソケットによる通信路に形成された仮想通信路の１つを割り当て、該仮想通信路によりプロセス81210とプロセス82210との間での通信を許可する
S807
通信を許可しない

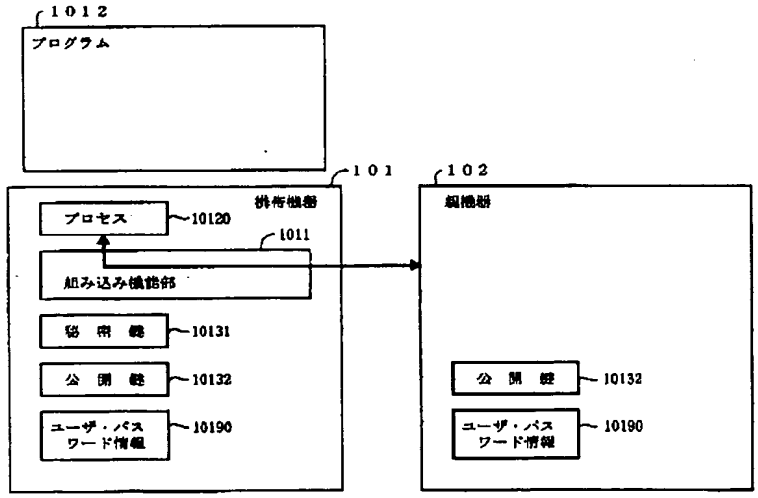
【図18】


S901
携帯機器91は、組み込み機能部911により、各ハッシュ値91231～9123nがプログラム本体9121および公開鍵群91221～9122nと各公開鍵91221～9122nと対をなす各秘密鍵とによって生成されたものであるかどうかを確認し、確認したハッシュ値に対応する公開鍵の集まりを得る
S902
親機器92も、組み込み機能部921により、各ハッシュ値92231～9223nをプログラム本体9221および公開鍵92221～9222mと各公開鍵92221～9222nと対をなす各秘密鍵とによって生成されたものであるかどうかを確認し、確認したハッシュ値に対応する公開鍵の集まりを得る
携帯機器91内のプログラム912を実行するプロセス9120と、親機器92内のプログラム922を実行するプロセス9120との間で通信要求発生
S903
S904
携帯機器91に付随する秘密鍵9131および公開鍵9132と、親機器92に付随する秘密鍵9231および公開鍵9232とにより相互認証
認証失敗
認証成功
S905
ハッシュ値確認結果の公開鍵の集まりをお互いに相手に伝え、一致する公開鍵があるかどうかを判定
不一致
一致
S906
プロセス91210とプロセス92210との間で通信を許可する
S907
通信を許可しない

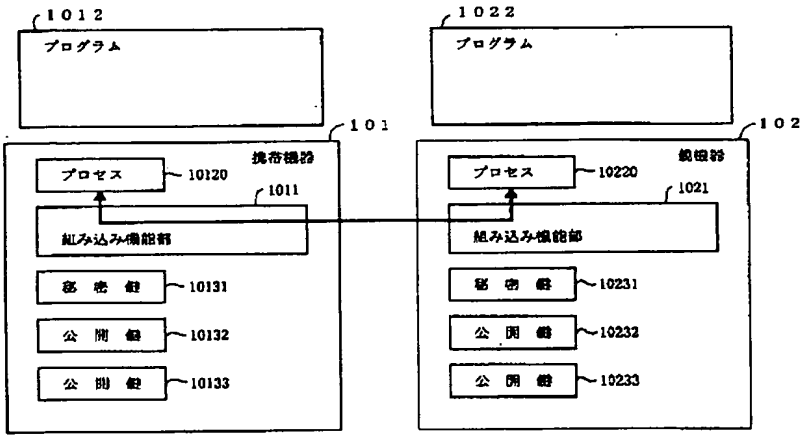
【図19】


1012
プログラム
101221～10122n
101241～10124n
公開鍵
秘密鍵
10121
プログラム本体
101
携帯機器
プロセス
10120
1011
組み込み機能部
102
相機器

【図20】


1012
プログラム
101
携帯機器
プロセス
10120
1011
組み込み機能部
秘密鍵
10131
公開鍵
10132
ユーザ・パスワード情報
10190
102
相機器
公開鍵
10132
ユーザ・パスワード情報
10190

【図21】


1012
プログラム
1022
プログラム
101
携帯機器
プロセス
10120
1011
組み込み機能部
秘密鍵
10131
公開鍵
10132
公開鍵
10133
102
機器
プロセス
10220
1021
組み込み機能部
秘密鍵
10231
公開鍵
10232
公開鍵
10233